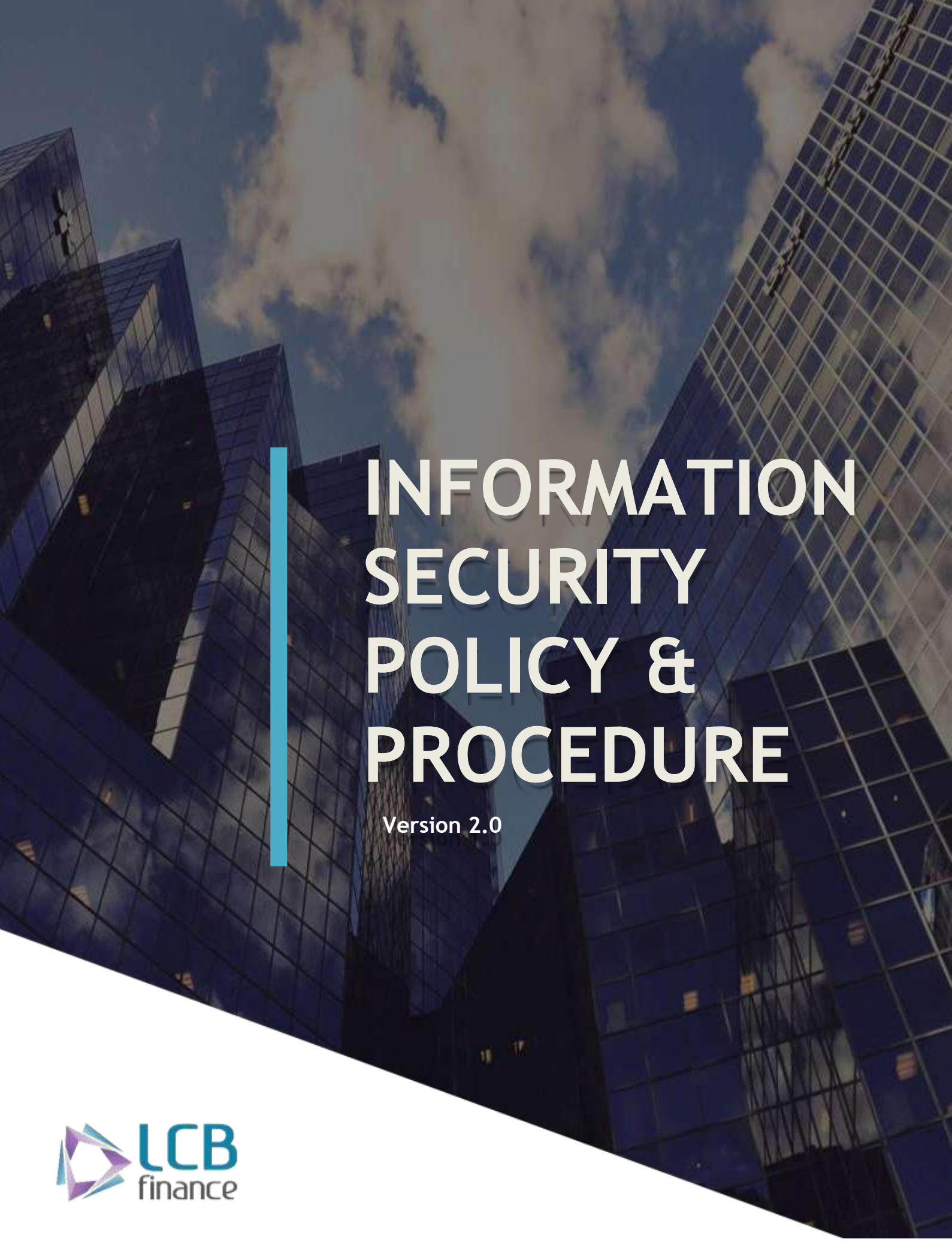

INFORMATION SECURITY POLICY & PROCEDURE

Version 2.0

LCB finance

Lanka Credit and Business Finance PLC

ISMS POLICY & PROCEDURES STATEMENT

It is the IT policy of Lanka Credit and Business Finance, PLC that its' information assets shall be protected from all threats identified, whether Internal or External, Deliberate or Accidental, such that the brand is protected; Confidentiality of Information is maintained; Integrity of Information can be relied upon; availability of information is ensured; and all legal, regulatory, statutory and contractual obligation are met.

MESSAGE FROM THE CEO/EXECUTIVE DIRECTOR

Lanka Credit and Business Finance, PLC recognizes that information is a critical asset and has become a business enabler in the industry. However, in this changing landscape, the level of risks to information assets is dynamically transforming. As we work towards our vision of being the preferred choice for creating wealth and value, we must always keep paramount in our minds the importance of fostering customer confidence by protecting the organisation's information assets from loss, theft, destruction, unauthorized modification and unauthorized access. Accordingly, Lanka Credit and Business Finance, PLC hereafter referred to as LCB Finance is committed to the implementation of Information Security by establishing comprehensive management processes.

To ensure successful & profitable operations, this Information Security Policy has been drawn up to set out the Management strategy which will in turn address Information Security concerns and the responsibilities of employees to prevent breaches of security thereby protecting our business. You will be aware that your contract of employment requires you to maintain confidentiality of the organisation's information. This requirement extends to protecting the entity's information stored on computer systems and hence you are responsible for the integrity of such information whilst in your possession. We will provide the necessary guidance and support to ensure that this Information Security Policy is successfully implemented.

We trust you would extend your fullest co-operation in this endeavour.

Best Regards,
Yours sincerely,

CEO / Executive Director

DOCUMENT DETAILS

DOCUMENT PROPERTIES

Document property	
Title	Information Security Policies & Procedures
Version number	Version 1.0
Classification*	INTERNAL – Confidential
Date	03rd of August 2022
Owner	Head of IT
Authorisation*	[To be Authorized]
Authorisation date	[To be Authorized Date]
Status	Final

VERSION MANAGEMENT

Version	Date	Author	Nature Of Amendment
Version 2.0	2024-06-01		Review and fine tune all Policies and Procedures

DISTRIBUTION LIST

NAME	VERSION	DATE

APPROVAL LIST

REVIEWER (ASSESSMENT)

NAME	VERSION	DATE

ASSESSOR (APPROVAL)

NAME	VERSION	DATE OF APPROVAL

TABLE OF CONTENTS

INTRODUCTION

Lanka Credit and Business Finance, PLC hereafter referred to as LCB Finance, has an obligation to clearly define requirements for the use of its information technology (IT) facilities and its information systems (IS) to all employees and business partners. LCB Finance (LCB) information technology resources constitute a valuable asset that must be managed accordingly to ensure the integrity, security, and availability for business activities. Carrying out this mission requires the organization to establish appropriate Information Security policies and standards so as to provide information system access and Security at an acceptable cost.

The objective of this requirement is to ensures that users of IT/IS facilities do not unintentionally place themselves, or the company, at risk of prosecution or disciplinary action, by carrying out computer related activities which contravene current policy or legislative restrictions. Information within the company is intended to be openly accessible and available to all members of the company for sharing and processing. Certain information (sensitive information) has to be processed, handled and managed securely and with accountability. This policy outlines the control requirements for all information contained within the company network and IT systems.

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of LCB Finance which must be managed with care. All information has a value to the Company.

Information Security controls are designed to protect members of the Company and the Company's reputation through the preservation of:

- Confidentiality - knowing that key data and information can be accessed only by those authorized to do so
- Integrity - knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version
- Availability - knowing that the key data and information can always be accessed.

The Company is committed to protecting its members and Key Business Systems. Controls will therefore be deployed that mitigate the risk of vulnerabilities being exploited which adversely affect the efficient operation of the Company.

Best practice policies and standards result in efficient, accountable and cost-effective use of resources. Information Technology Service (ITS) department is responsible for the corporate management of information and information technology. ITS department develops, proposes, and maintains IT policy, procedures and standards, and evaluates compliance. Areas associated with this authority include data access, electronic identity management, records management, information management, information technology, privacy, security applications, and systems of the organization.

The principles underlying effective managements are:

a) Information is a vital LCB asset that must be managed and, where appropriate, shared to maximize investments;

b) Information and technology are key components in delivering cost-effective services to the organization and public;

c) Information Technology has the potential, when planned and managed properly, to improve productivity and reduce costs to the organization;
d) Information and technology are strategic enablers of quality service delivery;
e) The outsource vendors from private sector is to play a major role in supplying services for the development and support of information technology.

PURPOSE

The purpose of this comprehensive document is to establish the framework governing information security within LCB Finance, and to establish an Information Security Management System (ISMS) within the organization.

SCOPE

The Information Technology Security Policies & Procedures [ISP] is applicable to all information assets of the entity. An Information Asset is a definable piece of information, stored and/or processed in any manner, which is recognized as valuable to the business. The types of Information Assets could be Software Assets, Physical Assets, Paper Assets, People Assets and Information Assets are Physical assets, Services Assets, People Assets and Information Assets that are physically or electronically stored, processed and/or transmitted by any of the aforesaid types of assets.

The ISP is applicable to all Employees of and Suppliers of LCB Finance. As a reference to this document, a service provider is called a Supplier only after Association with entity. These Suppliers might direct contracts with LCB Finance for providing products or services. They also include vendors who may have outsourced or sub-contracted the delivery of products/services that are required to be provided to LCB Finance Suppliers include IT Service Providers, Sub-Contractors and other Consultants/ Representatives of the above-mentioned Suppliers.

The term "Supplier Staff" mentioned in this document refers to the employees, agents, consultants and representatives of all Suppliers who are in any way accessing, processing, storing or transmitting any information assets of LCB Finance. The Information Technology Policy is applicable across all divisions and units of LCB Finance and across all geographies where the Information Assets of the entity is located.

ISMS POLICIES

IT POLICY

STRUCTURE OF DOCUMENT

This information security policy describes 'WHAT' to protect and sets the mandatory controls. At lower levels, more detailed descriptions of the approach and specific security measures are given. Specific handbooks define for each main process 'HOW' the rules shall be applied and how measures are implemented, managed and documented.

This Information Security Policy is designed to be in line with the LCB Finance information security policies and standards. It is based on management statements, critical success factors and generic rules.

GENERAL MANAGEMENT STATEMENTS

With this Information Security Policy, LCB Finance formally accepts ownership and responsibility for implementing and maintaining information security and risk management for all services provided and with regards to all data created, processed and received for internal business processes and client engagements.

LCB Finance shall:

- Assign someone to an information security role within the firm, who directly reports to senior management
- Perform periodical self-assessments on information security and risk management, and provide LCB Finance Global IT with requested 'Compliance Validation' information regarding the mandatory controls set out in this policy
- Have an accredited third party perform an external review of its information security controls
- Measure the effectiveness of the mandatory controls and critical success factors (CSFs)
- Initiate activities for improvement of information security based on the (self) assessments and continuous monitoring results
- Have documented security standards and procedures in place for monitoring digital security compliance across the organization, and make them available and accessible to relevant employees.

RESPONSIBILITY

Authorized Users of LCB Finance information technology resources are personally responsible for complying with all LCB policies, procedures and standards relating to Information Technology.

POLICY OWNERSHIP

Approved management responsibility for the development, review, and evaluation of the IT Manual for ensuring its continuing suitability, adequacy, and effectiveness is with Head of IT of LCB Finance PLC.

DEFINITIONS

a) Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.
b) Integrity: Data or information has not been altered or destroyed in an unauthorized manner.
c) Availability: Data or information is accessible and usable upon demand by an authorized person.
d) Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.
e) Information Assets: Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversation and over the telephone.
f) Business Continuity Planning: Business Continuity Management should be implemented effectively to ensure continuity of business operations in the event of a crisis or disaster.
g) Information Security Awareness: Ensure that relevant and effective Information Security Awareness trainings are provided to staffs.
h) Regulatory and Legislative Requirements: This will ensure that the organization remains compliant to relevant business, national and international laws and it include meeting the requirements stated in legislations

POLICY STATEMENTS

Controls will be deployed to reduce the risks of human error, theft, fraud, nuisance or malicious misuse of facilities. IT department maintains the directory of people and accounts which are authorized to use the company network, IT Services and applications. All users are subject to the principles of this policy and must certify that they agree to the terms, conditions and any other policy that this policy directly or indirectly related to. Security roles and responsibilities will be included in job descriptions where appropriate. These will include any specific responsibilities for the protection of particular assets, or the execution of particular processes or activities such as data protection.

All data which identifies any individual will be handled in accordance with the Data Classification Policy. All personal details will be held securely and in accordance with current company policy. All data transfers should follow the current recommendations in the Data Classification Policy and Access Control Policy. All data classified as Sensitive Data will be processed and stored in compliance with the current Data Classification Policy and company policies and procedures.

All entities are reminded of their obligation to protect confidential information in accordance with the company standard terms and conditions. All users will be bound by the confidentiality agreement in either their contract or terms of employment.

Security Incidents

- Suspected Security Breach

Users using the Company network or IT Services must not in any circumstances try to prove or collect evidence in relation to any suspected or perceived security breach. The exception to this rule is where staff has been granted a specific policy exemption which allows them to do so as part of their role. IT department will be responsible for identifying members of staff who are responsible for security breach investigations. A security incident is any incident which alters, destroys or amends data within the Key Systems without authority. May cause damage to or reduces the efficiency of the Company network or IT Services. This includes any actions or behavior which contravenes Company policy, statutory or common law legal requirement or professional regulation or guidance.

- Reporting Security incidents

All suspected security incidents are to be reported in the first instance to the IT department. Initial reports of suspected security incidents should be channeled through their department/branch to the IT department. The IT department system will be used to record suspected security incidents through the network. Unless the initial risk assessment indicates that such a recording process will put the investigation in jeopardy or alert the persons involved in criminal activity. All reported security incidents and active investigations will be monitored by the proper authority. An appropriate investigation and action plan will be prepared and agreed with a representative of the Company Management.

The Company reserves the right at any time to intercept and monitor communications. The above legislation will be implemented in compliance with the monitoring provisions contained within the Acceptable Use Policy, Access Control Policy Monitoring and recording of electronic communication and data will be carried out in accordance with current Company policy and interception/monitoring of individual activity shall normally only take place with the prior express approval of the proper authority, but may be undertaken without any prior notice to the users of Company systems.

Permission for undertaking monitoring or surveillance of user activity may in the first instance be given verbally; any such permission must be recorded in writing as soon as practicable, this requirement is to ensure an auditable investigatory process exist for any subsequent disciplinary or criminal proceedings.

- Security Incident Management/Investigation

The senior member of staff identified as being responsible for investigating the incident will ensure that all steps are taken to limit damage and loss of data whilst preserving the reputation of the Company. The IT department will maintain written procedures for the operation (e.g. start up, backup, shut down and change control) of those Company Key Systems where threat, risk and organizational impact would adversely the operational effectiveness or organizational reputation.

- Investigating Information Security Incidents

On receipt of information indicating that a security incident may have taken place the Manager IT will inform the HR Department and a member of staff will be nominated to coordinate the investigation. The investigation will follow the company Information Security Procedure.

- Network Isolation and Reconnection

Any device perceived as placing the integrity of the Company IT network at risk to harm or service interruption will be isolated from the main network domain. Suspension of network connectivity will remain in force until the issue has been investigated and a plan of action agreed with the Head of the IT department to resolve the issue. Subsequent reinstatement will only be permitted once the requirements of that action plan have been met, verified and authorized by the Manager IT.

Physical and Environmental Security

Design build and configuration documentation will be produced in respect of system platforms. Sensitive documentation will be held securely, and access restricted to staff on a need to know basis.

- Physical Security

Computer systems and networks will be protected by suitable physical, technical, procedural and environmental security controls. File servers and machines that hold or process high criticality, high sensitivity or high availability data will be located in physically secured areas. All Key Systems will be subject to security measures which supports the Company policy.

Servers holding corporate information will be held in a secure environment protected by:

- Physical security and access control
- Fire detection and extinguishing systems
- Temperature and humidity control
- Water sensors
- Stable, conditioned electrical supply protected by uninterruptible power supply (UPS) and standby generator

Company electronic information will be held on servers approved by IT department. External hosting must not take place without prior approval from the IT Department. Key communications equipment will also be protected by UPS

IT department must ensure the IT Infrastructure is covered by appropriate hardware and software maintenance and support.

Workstations must be appropriately secured and operated by Company employee who must be trained in and fully conversant with this policy or any other policy and their personal responsibilities for confidentiality of information displayed on the screen or in printed output.

Backup media must be retained in accordance with Company policy on retention of records and the Data Classification Policy.

All Company data must be cleared securely from Company IT equipment and media on disposal. All IT equipment must be disposed of via appropriate authority; this includes secure erasure and destruction of data. The responsibility for disposal lies with the company, with assistance from IT Department.

System Change Management

All changes to live Key Business Systems will follow a pre-defined change management process, to ensure that activities are undertaken in accordance with stringent change control processes.

Controls against Malicious Software

- Controls will be implemented to check for malicious or fraudulent code being introduced to Key Systems.
- All systems will be protected by a multi-level approach involving firewall, router configuration, e-mail scanning, and virus and spy/malware protection on all workstations on the Company network.
- All Company workstations will have appropriate anti-virus software installed by IT department set up to update anti-virus Signatures automatically. This must not be turned off by users.
- Any device found to pose a threat to data or the provision of the Company network will be isolated from the Company network until the security issues are resolved.
- Network traffic will be monitored for any anomalous activity which may indicate a security threat to the network.

Virus Protection

A Virus Protection procedure will be implemented to prevent the introduction and transmission of computer viruses both within and from outside the Company. Failure to maintain a device in a state which prevents or detects virus infection will leave the device liable to exclusion from the Company network until the security issue is resolved.

Security Patches Fixes and Workarounds

Patches, fixes and workarounds must be tested and approved before deployment and the efficiency of the deployment will be monitored to ensure the effective mitigation of risk due to known vulnerabilities.

Data Backup & Storage Management

System backups will be performed by the relevant user in accordance with procedures. The procedure will include keeping backups off site in secure storage. Periodic checks will be made to ensure backup media can be read and files restored. Records of backups will be monitored by IT department and be subject to random audit by the company representative. Backups of corporate data are taken on Key Business Systems or less frequently if appropriate. Backups protect electronic information from major loss or failure of system software and hardware. Backups are not designed to guard against accidental deletion or overwriting of individual user data files Backup and recovery of individual user files is the responsibility of the owner.

Network Management

Controls will be implemented to achieve, maintain and control access to computer networks, including wireless networks. The configuration of critical routers, firewall and other network security devices will be the responsibility

of, maintained by, documented and kept securely by the IT department. No IT equipment with the exception of authenticated mobile devices may be connected to the Company network without approval by IT department.
Any device found to be installed without prior authority from IT department will be disconnected, the equipment removed and an investigation commenced to establish the cause of the network compromise. Users should be aware that installation of such devices is potentially a disciplinary and criminal offence under the company policy.

Disposal of Information

Removable magnetic and optical media containing Key Business System data or Sensitive Information will be reused or disposed of through controlled and secure means when no longer required, in accordance with the relevant procedures. Redundant computer equipment will be disposed of in accordance with the relevant procedures and through secure and auditable means.

Procedures will be made available for the secure disposal of removable data storage media containing Key Business System data or sensitive information when these become defunct or unserviceable. Users should contact the IT department for the current procedures.

Software Usage and Control

Software will be used, managed and controlled in accordance with Company policy requirements in relation to asset management and license agreements. All major software upgrades and in-house systems development for Key Business Systems will be appropriately controlled and tested through a managed process before live implementation and deployment. All software used on devices managed by IT department must be installed in compliance with current software licensing policy and software deployment policy as specified by the IT department. Software installed without IT department authority and agreement may leave a user liable to prosecution under the company policy and disciplinary action.

Information Exchange Requests

Use of the Company network will be governed by the Access Control Policy and the Data Classification Policy. Failure to comply with these requirements will leave a user liable to disciplinary and/or possible criminal legal penalties.

- Exchange of Information with Outside Organizations

Requests by external bodies for the provision of electronic information From Key Business Systems will in all instances be referred to the system owner. This includes Data Subject Access Requests made under the auspices of the Access Control Policy. Responses to Data Subject Access Requests in respect of systems owned and operated by IT department will be coordinated by the Manager IT Department.

- Guest Users and Open Access

Guest user accounts and open access facilities may be used to allow visitors strictly limited access to the company network. Written records of such IT use (who, when and where) must be maintained by the IT department. Access to corporate systems, protected electronic resources, company e-mail services and personal file store will not be permitted unless there are special circumstances.

- Subject Access Management and Administration

Formal procedures will be implemented for granting access to both the company network and IT Services. This will be supported by a formal review of user privileges on a regular basis to ensure that they remain appropriate to the role and relationship with the company. Accounts identified as dormant accounts will be closed in accordance with current procedures.

- Remote Access

Controls will be implemented to manage and control remote access to the company's network and IT Services. Key Business Systems will have controlled access in accordance with the Access Control Policy and Data Classification Policy and Acceptable Usage Policy. Users should note that failure to comply with the Access Control Policy and Data Classification Policy and End User Computing Policy will leave the user liable to disciplinary action and possible criminal law prosecution under the appropriate legislation.

Password Management

Users are required to follow good security practices in the selection; use and management of their passwords and to keep them confidential in accordance with the Acceptable Use Policy and Access Control Policy. IT department maintain procedures for the issue of and closure of user accounts. Authorization of access to Key Business Systems and to the data held by them is the responsibility of the system owner. The company aims to minimize the number of accounts required by each individual. The Control of network passwords is the responsibility of IT department. Network passwords are stored in encrypted form. Reissue of network passwords is through the IT department following a documented procedure. IT department maintains records of the issue of system administrator passwords and ensures they are stored securely. System administrator passwords will be issued on the express authority of the Manager IT on a need to know basis. Such passwords will be changed regularly and when authorized system administrator staff leaves.

IT department must be notified when staff leave and will be responsible for closing the associated accounts. Responsibility for retention of any files held by staff that leave lies with their company/service and should form part of their relevant procedure. Company and Services responsible for electronic information assets will be informed when staff authorized to access those assets leave and will be responsible for controlling access rights to those assets. Account type should at all times reflect the business relationship existing with the member of staff. As astaff member moves to a less formal relationship with the company then the account associated with that person should reflect this new relationship.

IT department will maintain a list of staff with access to key business systems and services. A password matrix will be maintained to ensure business continuity and mitigate risk. This password matrix will be kept securely to ensure swift response to critical incidents.

Monitoring Systems Access and Use

Access to and use of the company network and IT Systems will be monitored in accordance with the provisions of the relevant policies. Remote access by third party contractors to maintain and support company IT systems will be subject to appropriate monitoring and control measures defined by IT department. Third Party access will only be granted where the applicant has agreed to the terms and conditions of the Acceptable Use Policy, Access Control Policy and Data Classification Policy.

CONSEQUENCE MANAGEMENT FOR NON-COMPLIANCE

All employees and Suppliers are required to comply with the Information Security Policy (ISP). Non-Compliance with the ISP is ground for Consequence Management, up to and including termination, Disciplinary Procedures shall be invoked to deal with such non-compliance. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Exceptions

The ISP is intended to be a statement of Information Security Requirements that need to be met in the organization. The exception request, validation and management procedure should be formalized by the management. However, exceptions against individual controls in specific policy domains shall be formally documented in the Security Override Document (SOD) which will include at a minimum, the following:

a. Justification for the exception
b. Risk due to the exception
c. The mitigation controls to manage the risk
d. The plan of action to manage the risk
e. The Validity period of the exception
f. Details of assets on which the SOD is applicable

1.0. IT SECURITY POLICY

1.1. GENERAL MANAGEMENT OF IT SYSTEMS

Management Statement

LCB Finance shall be in control of access, changes, configuration and licensing of all infrastructure components used to access, store or create LCB Finance data.

Critical Success Factor

The embedded software (operating system or firmware) used to run infrastructure components is controlled (access, changes, availability, configuration), up-to-date with patches and supported by the vendor. Management of third party or cloud based services are controlled with the same processes and procedures.

1.1.1. ACCESS CONTROL

All access to systems and network components shall be controlled and managed.

1.1.1.1. Mandatory Controls

- All system, application and (privileged) user accounts are treated as an 'identity'
- LCB Finance systems and data can only be accessed through authorized and authenticated identities
- All authorization requests are controlled using the Joiner, Mover, Leaver (JML) process (2.3)
- Access is granted based on the principles of *'need to have'* and *'least privilege'*
- All authorizations are reviewed periodically and adjusted immediately if required
- Administrative access is only granted on specifically created, personal user accounts
- Shared generic accounts are not used on business critical systems and applications
- Non-personal/shared generic accounts are only used if other measures are implemented to determine the (source) end-user
- All user accounts (identities) are traceable to a physical person
- An up-to-date and complete authorization directory storing all identities is used
- A documented password policy is applicable and enforced for all accounts in use
- Local accounts are only used if account control and password requirements are met. Cloud based access is always configured with multifactor authentication.

1.1.2. OPERATING SYSTEMS

All systems and network components shall run on licensed and vendor supported software and firmware. Security measures shall be controlled and managed.

1.1.2.1. Mandatory Controls

- All workstations used for business or containing business/client data shall run on an Operating System that is still supported by the vendor/manufacturer and that will not go out of support within 12 months at any given time
- All servers, endpoints and network equipment are set-up in the same manner for providing basic functionality (baseline setup) and only offer additional functionality and services that are specifically required for the system role
- Additional software is made available for installation in a controlled manner and only after approval and testing
- All production servers and applications are checked periodically on compliance with the baseline:
    - Logging is enabled on all servers and is proactively reviewed
    - All unused accounts and services are removed or disabled
    - All unrequired services are be disabled
    - All user/services access to the systems are least privileged
    - Anti-virus software is installed and configured to be updated and report events
- Security patches are installed as soon as possible, but not later than 30 days. Critical and/or out-of-band patches are installed as soon as possible
- All installed applications are commercially available and/or (vendor) supported.

1.2. INFRASTRUCTURE POLICY

Management statements

All network entry/exit points shall be protected and controlled with industry standard firewall(s) and shall allow only connections that explicitly match the approved connectivity rules.

Detection mechanisms and procedures shall be in place to protect the infrastructure from internal and external digital treats and to respond effectively to a cyber security incident.

Critical Success Factor

The infrastructure is protected with firewall equipment for both internal and external network traffic. Network traffic is monitored against known threats and network events and logfiles are stored.

1.2.1. FIREWALL MANAGEMENT

Firewalls are critical components in protecting infrastructure. Next to controlling the embedded software, additional rules for firewall management apply.

1.2.1.1. Mandatory controls

- Network segmentation is implemented to ensure trusted and untrusted networks are separated
- Documented processes/procedures for firewall management:
    - Creating, changing and removing firewall rules is controlled by a change management process
    - Firewall rules are specific to the required source and destination addresses and services rather than wide ranged
    - The firewall ruleset is reviewed periodically, but at least every 12 months
    - Firewall event logs are reviewed periodically and deviations are treated as a security incident
    - Firewall maintenance (including applying updates) is performed by operational procedures and controlled by a Change management process
    - The firewall has additional functionality to detect malicious traffic and blocks this automatically
    - The detection capability of malicious traffic is updated automatically and applied to at least all internet and email traffic.

1.3. SERVER MANAGEMENT

Management statement

LCB Finance shall ensure all servers are protected with adequate malware protection and that vulnerabilities on systems are proactively and effectively identified and appropriate actions are taken.

Critical Success Factor

LCB Finance ensures all servers have malware protection solutions installed, configured and running, and that known vulnerabilities are periodically proactively and effectively identified, classified, remediated and mitigated. This cyclical process is documented in an operational procedure.

1.3.1. MALWARE PROTECTION

All servers shall run on licensed and vendor supported software and firmware. Security measures shall be controlled and managed.

1.3.1.1. Mandatory controls

- All servers have a malware protection solution installed and running.
- Malware protection on servers is centrally managed.
- Forced software updates are applied to all servers as soon as new releases are available within an acceptable timeframe, but at least on a monthly basis.
- Real-time scans of active content are in place and scans of servers are configured on a weekly basis (as a minimum).

- Externally uploaded data to LCB Finance file sharing services is scanned for malware before it is made internally distributed.

1.3.2. VULNERABILITY MANAGEMENT

All vulnerabilities on systems shall proactively and effectively be identified and appropriate actions shall be taken.

1.3.2.1. Mandatory controls

- Vulnerability management policies and procedures are in place
- Vulnerability scans run across servers periodically
- All external facing infrastructure shall be subject to (at least) annual penetration testing, or with every major change
- A risk classification matrix is used to discover and classify vulnerabilities on servers
- Appropriate action on identified risks is taken following Change management procedures.

1.4. END-USER DEVICES

Management statement

LCB Finance shall ensure all devices used by employees to access, store and/or process LCB Finance classified data are secured appropriately.

Critical Success Factor

LCB Finance ensures all end-user devices in use have vendor supported malware protection installed and running, and are secured by real-time scanning of active content and shall quarantine suspicious content. Operational procedures for follow-up exist.

1.4.1. ENCRYPTION

All classified data on information systems shall be encrypted by vendor supported and industry standard encryption.

1.4.1.1. Mandatory controls

- Procedures are in place for encryption key management
- (Master) Keys are kept secure at all times
- All LCB Finance data 'at rest' is encrypted using full hard disk encryption applied on all end-user devices, using vendor supported industry standard encryption
- A procedure is in place to recover data from encrypted devices
- Appropriate hardware is used that enables applying vendor supported industry standard encryption

- All LCB Finance classified data 'in transit' is encrypted.

1.4.2. MALWARE PROTECTION

All end-user devices shall be protected with adequate malware protection.

1.4.2.1. Mandatory controls

- All end-user devices are equipped with vendor supported malware protection, including but not limited to virus, spam and spyware
- Forced malware protection updates are applied to all end-user devices daily
- Real-time scanning of active content on end-user devices is configured weekly
- Malware protection on end-user devices is centrally managed.

1.4.3. MOBILE DEVICE MANAGEMENT

LCB Finance shall recognize all privately owned devices used by employees (laptops, tablets, smartphones, etc) used for storing, accessing and/or processing of data as a ‘mobile device’.

All LCB Finance classified data accessible for, and stored on, a mobile device shall be protected against unauthorized access.

1.4.3.1. Mandatory controls

- Documented processes/procedures are in place for mobile device management covering:
  - A documented registration process for all mobile devices
  - An explicit privilege/access right for the use of a compliant mobile device is only granted after successful registration and a successful device compliance check
  - Compliance status of operating systems, changes to default security settings and anti-malware settings on all mobile devices are periodically checked
  - Procedures to force end-users to grant administrative access to the mobile device and allow LCB Finance to (partially) manage mobile device settings or perform remote wiping.

2 GOVERNANCE POLICY

2.0. INFORMATION SECURITY & RISK MANAGEMENT

2.0.1. Management statement

LCB Finance shall ensure that Confidentiality, Integrity and Availability of all LCB Finance information, services and client engagements are appropriately safeguarded and controlled, by integrating information security and risk management in the business-as-usual routines throughout all levels within the firm.

2.0.2. Critical Success Factor

LCB Finance has a formally approved information security policy (this document) that is implemented in the organization using documented procedures for applying information classification, performing risk assessments, performing security testing and designing security controls and measuring their effectiveness. A documented security incident management process and exception process is also implemented. Formally approving the information security policy is reserved for only.

2.0.3. Mandatory Controls

- Business critical systems and processes are identified
- Business critical systems and process owners are identified and responsibilities are clearly defined and approved
- For each critical system and process, the business impact of loss of Confidentiality, Integrity and Availability is assessed every two (2) years, or in the event of major changes
- User activity and system events on business critical systems and processes are logged and monitored
- The effectiveness of each control protecting the Confidentiality, Integrity and Availability is tested annually
- A risk log to register risks and exceptions on policies and controls, accepted by, is available, complete and up-to-date
- A procedure for registration and handling security incidents is available and approved by senior management. It includes performing a mandatory root cause analysis and implementing improvements for all high-impact security incidents.

2.1. INFORMATION RISK TREATMENT

2.1.1. Management statement

LCB Finance shall ensure that appropriate controls and processes are in place to effectively and continuously identify, (re)evaluate and treat information risks according to the accepted risk level. Formally accepting (residual) risk is reserved for senior management only and is reviewed yearly or earlier in the event of changing circumstances. The use of cyber security insurance is allowed, but shall not limit the requirement for implementing controls for lowering impact or likelihood of a risk.

2.1.2. Critical Success Factor

LCB Finance has a documented process to ensure information risks are effectively and continuously identified, (re)evaluated, and treated in accordance with the accepted risk appetite. A risk profile is established.

2.1.3. Mandatory Controls

- Established and accepted risk levels are identified and in line with risk profile
- Procedures are in place to identify, evaluate and treat identified risks
- Procedures are in place to identify and document residual risk
- For each critical system, information risk treatment plans are developed.

2.2. PEOPLE MANAGEMENT

2.2.1. Management statement

LCB Finance shall ensure all people with access to LCB Finance offices, systems and/or information are suitable for their role(s), access and authorizations are provisioned role-based, and employees know their information security responsibilities.

2.2.2. Critical Success Factor

LCB Finance ensures all people with access to LCB Finance offices are aware of their roles, responsibilities and the risks involving information security and that their user accounts are aligned with current roles and responsibilities.

2.2.3. USER PROVISIONING

All user accounts are personal and are at all times aligned with the current duties, roles, responsibilities and employment status of all employees.

2.2.3.1. Mandatory Controls

- User management processes for Joiner, Mover, Leaver (JML process) and controls to service (de)provisioning and delegation of user accounts are aligned with HR's starting, changing or terminating employment processes
- Procedures to carry out background verification checks on all candidates for employment. These are in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed and the perceived risks
- Service provisioning and delegation of user accounts is initiated from the HR process
- Procedures to ensure all employees return LCB Finance 's equipment (such as mobile devices), access cards, tokens, etc.

2.2.4. AWARENESS AND TRAINING

All employees are at all times demonstrable sufficiently trained and aware of their roles, responsibilities and the risks involving information security.

2.2.4.1. Mandatory Controls

- Appropriate ongoing awareness education and training, and regular updates in organizational policies and procedures for all employees, as relevant for their job function, are in place
- Procedures to periodically assess the current level of security awareness of all employees, such as phishing tests or security awareness tests are in place

- Procedures to facilitate, record and measure periodic training activities to increase security knowledge of key users about high risk systems are in place.

2.4. BUSINESS CONTINUITY/CRISIS MANAGEMENT

2.4.1. Management Statement

LCB Finance shall take measures to ensure the continuity of core business processes, to meet client expectations and to comply with legal and regulatory obligations. Identifying and mitigating continuity risks shall be embedded in the business impact assessment process.

2.4.2. Critical Success Factor

LCB Finance has up-to-date, documented and tested business continuity and disaster recovery plans focussed on restoring core business processes and systems within accepted timeframes during a calamity or crisis.

2.4.3. Mandatory Controls

- Processes are in place to identify business continuity risks, which at least include procedures to:
  - Identify all critical business processes and map all business processes and systems
  - Perform Business Impact Analysis (BIA) for each business application to determine the business accepted risks
  - Assess all potential damage encountered through security incidents
- Procedures are in place to prioritize business continuity risks, such as procedures to:
  - Determine the Maximum Tolerable Downtime (MTD) for all critical systems and business processes
  - Determine the Recovery Time Objective (RTO) for all critical systems and business processes
  - Determine the Recovery Point Objective (RPO) that is aligned with LCB Finance ’s backup policies
- Procedures are in place to test business continuity and disaster recovery plans annually
- A back-up policy that meets the availability requirements (MTD, RTO and RPO)
- Procedures are in place to test a full restore for all business critical systems at least bi-annually.

2.5. IT SERVICE MANAGEMENT

2.5.1. Management Statement

LCB Finance shall ensure a controlled process for managing the entire lifecycle of information systems used to access, store and/or process LCB Finance data.

2.5.2. Critical Success Factor

LCB Finance has operational procedures in place to manage and control the entire IT infrastructure using generic IT service processes for handling incidents, changes and problems.

2.5.3. Mandatory Controls

- Generic IT Service processes regarding Configuration, Incident, Change, and Problem management are in place
- Performance and capacity monitoring and follow-up processes are in place for all business critical systems and processes
- Documented procedures are made available and accessible for all employees involved.

2.5.4. CONFIGURATION MANAGEMENT

2.5.4.1. Mandatory Controls

- All systems and network components are identified and centrally registered before being elevated to production status in a Configuration Management Database (CMDB) or equivalent registration
- Procedures exist to keep the CMDB accurate and up-to-date.

2.5.5. INCIDENT MANAGEMENT

2.5.5.1. Mandatory Controls

- A documented incident management process is available and up-to-date
- Security related malfunctions and service requests (requiring access, connectivity, restoring of backups, functionalities, etc) are registered in a centrally managed system and assigned a unique ID
- Tickets/requests are routed to the appropriate solver or authorization group
- All actions shall be logged under the original and unique ticket number.

2.5.6. CHANGE MANAGEMENT

2.5.6.1. Mandatory Controls

- A documented Change management process is available and up-to-date.
- All changes to production systems and applications shall be controlled and managed following the Change management process.

- Security patches are applied according to the Patch management process and treated as a (standard) change.

2.5.7. PROBLEM MANAGEMENT

2.5.7.1. Mandatory Controls

- A documented procedure is in place to investigate the root cause of major incidents and control the restoring of functionality of all (reoccurring or) high impact incidents.
- Known issues and fixes are documented.

2.6. THIRD PARTY SECURITY

2.6.1. Management Statement

LCB Finance shall ensure all LCB Finance data processed by third parties or stored on third party systems is protected against unauthorised access, changes or deletion. Appropriate measures shall be taken to comply with (inter)national laws and regulations in case third parties abroad are used.

2.6.2. Critical Success Factor

LCB Finance ensures all externally stored data is owned and controlled and that all third party processors act according to LCB Finance security policies and applicable (inter)national laws and regulations.

2.6.3. Mandatory Controls

- A countersigned agreement with a detailed service description is available (master agreement)
- Additional agreements with third parties on security requirements and Service Level Agreements (A) metrics are included in the master agreement
- A documented procedure exists to classify and manage all externally stored LCB Finance data
- Documented procedures exist to ensure risks directly related to the use of external services are identified and mitigated to an acceptable level
- Periodic audits or reviews to assess whether the third party is compliant with LCB Finance policies and standards are carried out.
-

2.6.4. OUTSOURCED SERVICES

Additional rules for the use of outsourced services apply.

2.6.4.1. Mandatory Controls

- The outsourcing partner has a service catalogue that describes provided service(s)

- The outsourcing partner has documented procedures for delivering the service to LCB Finance
- LCB Finance receives a monthly report regarding the the delivery of the provided service(s), based on the A.

2.6.5. CLOUD PROVIDERS

Additional rules for the use of cloud providers apply.

2.6.5.1. Mandatory Controls

- The type of cloud (private/public/hybrid) is applicable for the intended use and type of data to be stored/processed. This is in line with (inter)national laws
- The cloud provider complies with agreements on the disposition, deletion and recovery of data
- The cloud provider has a service catalogue that describes the services. Documented procedures are used for delivering the service to LCB Finance
- LCB Finance receives insight about the use of the service, based on the A metrics
- The cloud provider ensures and proves that LCB Finance data is protected according to LCB Finance security policies and (inter)national laws and regulations, such as contractual agreements on data portability and extraction

All mandatory, additional and elevated technical measures imposed by the LCB Finance Risk Management Manual are described in this chapter from the viewpoint of infrastructure, servers and/or end-user devices. Generic security measures, applicable for each system type, regarding system management are detailed in the next section.

2.6.6. COMPLIANCE MONITORING

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department.
Violations of the policies, standards and procedures of Certis will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department.

IT STANDARD OPERATING PROCEDURE

1. INFORMATION SECURITY AND RISK MANAGEMENT

PURPOSE

This publication seeks to assist organization by providing a document of minimum standards regarding the use and management of IT Security & Risk Management within the entity. This standard and procedure must be used to provide a methodology to comply with applicable policies. The purpose of this policy is to help the entity establish security requirements in order to have a risk weighted controlled access to the information resources of LCB Finance to ensure accuracy, confidentiality, and availability of information. This document also provides direction in identifying IT related risks and creating and maintaining a Risk Management Framework.

INTRODUCTION

This is documented to facilitate effective and efficient IT Strategic Plan implementation and establish IT Department involvement in relevant decision-making processes and provide direction to the management on the IT Strategic plan and its alignment with the business strategic objectives. The IT Strategic Planning is required to manage and direct all IT resources in line with business strategies and policies and implementing a Technology Infrastructure Plan that takes advantage of available and emerging technologies by which the business strategy shall be driven and facilitated.

SCOPE

This policy & procedure applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance regardless of the geographic location. This document covers all Information Systems (IS) environments operated by the entity and/or contracted with a third party by LCB Finance.

All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her systems administrator, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy.

OBJECTIVES

- To ensure all business-critical systems and processes/owners are identified and responsibilities are clearly defined and approved.
- For each critical system and process, the business impact of loss of Confidentiality, Integrity and Availability is assessed every 2 years or in case of major changes.
- The effectiveness of each control protecting the Confidentiality, Integrity and Availability is tested annually.
- To establish and maintain risk logs to store exceptions on policies and controls, accepted by senior management, is available and up to date.
- To ensure established and accepted risk level are identified and are in line with risk profile.
- To determine whether procedures are in place to identify, evaluate and treat identified risks.
- Procedures are in place to identify and document residual risk.
- To determine whether each critical system information risk treatment plans are developed.

- To ensure that a procedure for registration and handling security incidents is available and approved by senior management. It includes performing a mandatory root cause analysis and implementing improvements for all high-impact security incidents.

DEFINITIONS

Information Asset: Information Asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization.

Information Asset Owner: The information asset owner has the responsibility of classifying the asset on the basis of LCB's asset classification scheme and related guidelines. The owner of the information asset shall identify/approve the controls to be implemented to provide appropriate protection to the asset. In addition, the asset owner should annually review the access control policies and classification processes. The owner of the information asset is accountable for the security of the information asset.

Information Security Event: An information security event indicates that the security of an information system, service, or network may have been breached or compromised. An information security event indicates that an information security policy may have been violated or a safeguard may have failed.

Risk Assessment: Overall process of risk identification, risk analysis, and risk evaluation.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	IT Executive

SPECIFIC PROCEDURE

The Manager IT shall define the IT organization structure considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, supervision.

The Structure is to be embedded into the IT Process Framework that ensures transparency, accountability and controls as well as the involvement of senior executives and business line management.

The IT Steering Committee should ensure board oversight on IT and one or more steering committees, in which business and IT would participate, should determine prioritization of IT resources in line with business needs.

Processes, administrative policies and procedures need to be in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, individual accountability and segregation of duties. IT is to be involved in relevant decision-making processes, in order to ensure timely support on business requirements.

LCB Finance shall have an IT Strategic Plan that is aligned with the business strategic goals and objectives. The IT Strategic Plan shall improve key stakeholders' understanding of IT opportunities, limitations, assess current performance and clarify the level of investments required.

LCB Finance shall create and maintain a risk management framework. The framework documents a common and agreed level of IT risks, risk treatment plans, mitigation strategies and agreed-upon residual risks. Any potential impact on the goals of the organization caused by an unplanned event

shall be identified, analyzed and assessed. Risk mitigation strategies shall be adopted to minimize residual risk to an accepted level. The result of the assessment shall be understandable to the stakeholders and expressed in quantifiable terms, to enable stakeholders to align risk to an acceptable level of tolerance.

IT Process Framework

LCB Finance, shall define an IT process framework to execute the IT strategic plan. This framework includes a high-level process structure and relationship. It provides integration between the processes that are specific to IT and its linkage with enterprise portfolio management, business process management and business change management processes as applicable. The IT process framework shall be integrated with an IT quality management system and the internal control framework where IT is supporting the business processes.

An IT Steering Committee shall be formed to oversee the proper alignment of IT processes with Business goals and objectives, review and approve IT policies, procedures and projects and review strategic and tactical IT plans to ensure that they are in line with LCB Finance, strategic goals and objectives.

Associated procedure

An IT Steering Committee should be established officially by the Chairman with the assigned authority to approve IT and IS Policies. The IT Steering Committee should be composed of the Chairman; as the Chairperson, Director Finance, IT Consultant, Manager IT and the Technician. The Chairperson calls the IT Steering Committee's meetings as and when needed and if the Chairman is not available, Joint Finance & Economic Research will take his place. The IT Steering Committee should meet quarterly to review IT projects' progress, provide guidelines and feedback and take corrective/preventive actions if required.

The IT Steering Committee should consider inputs from all LCB Finance. Directors relating to comments and concerns regarding the entity's Information Technology.

For each meeting, the Manager IT should compile an IT Steering Committee's Progress Report in coordination with the committee members. The IT Steering Committee's Progress Report should include documented information regarding new systems projects and directions of the IT activities.

The IT Steering Committee should provide the Chairman with the IT Steering Committee's Progress Report within one (01) week subsequent to the IT Steering Committee's quarterly meeting is held.

All proposed changes to IT Policies and Procedures should be formally proposed by the Manager IT, reviewed by the IT Steering Committee and should be approved by the Chairman.

Organizational Placement of the IT Function

The IT function shall be incorporated into the overall organizational structure with a business model contingent on the importance of IT within LCB Finance, specifically considering the effective criticality to business strategy and the level of operational dependence on IT.

The Director Finance and Department Heads shall be responsible to ensure that the IT Policies and Procedures are adhered to and followed by as approved by the IT Steering Committee.

Associated procedure

The reporting line of the Manager IT is commensurate with the importance of IT within LCB Finance, as such the Manager IT should be reporting directly to Joint Finance & Economic Research.

Roles and Responsibilities

The Manager IT & Director Finance shall define roles and responsibilities for all LCB Finance employees in relation to IT Department's information systems.

Associated Procedure

The IT Department should communicate IT related roles and responsibilities to all employees to allow sufficient authority to exercise the roles and responsibilities assigned to them.

Additionally, The IT Department should define the expectations of each role or responsibility and this information should be provided to employees with respect to their roles and responsibilities and obtain official consent of understanding from each employee.

Once employees sign for the consent of understanding they immediately assume responsibility of acting in accordance with the IT assigned roles and responsibilities. The IT Department should bi-annually review the assigned roles and responsibilities to meet business objectives and address the changing circumstances and accordingly update and communicate such new changes to affected parties.

In addition to communicating updates and changes, the Manager IT should bi-annually assess the performance of the employees in relation to IT Department's information systems with respect to their roles and responsibilities.

Business-IT Alignment

The IT Steering committee shall ensure that effective and efficient enabling IT technologies to business goals and objectives are evaluated and selected. The IT Steering Committee shall educate other executives on current technology capabilities and future directions, the opportunities that IT provides and what the business has to do to capitalize on those opportunities.

Associated Procedures

The IT Steering Committee is responsible for developing and owning the IT Strategic Plan. The maintenance of this plan will be the responsibility of Manager IT. Accordingly, the committee should hold an annual meeting to review the Business Strategic Plan. This meeting is to be conducted shortly after the compilation of the Business Strategic Plan. The Director Finance should call and attend this meeting. The IT Steering Committee should review the Technology Infrastructure Plan's implementation to ensure that the goals and objectives are correctly incorporated and addressed.

Assess IT Capability Current Status

The current status of the IT Infrastructure at LCB Finance shall be assessed annually prior to the IT Strategic Planning process takes place. The IT Capability Current Status assessment shall form the basis for the IT Strategic Planning.

Associated Procedures

The IT Steering Committee should annually assess LCB Finance's current IT Infrastructure within 3 months period based on the following parameters:

- Extent of automation of business processes and degree of functionality of the systems
- The complexity of the IT environment
- The scalability of the IT components employed
- Capacity planning and sizing of key hardware components
- Transaction handling adequacy and capability of the key applications
- The infrastructure improvement costs and running costs
- Measures in place to deal with IT Contingencies
- Strengths, Weakness, Opportunities and Threats (SWOT) Analysis on technology environment.

Upon concluding the current IT infrastructure assessment, the IT Steering committee should via the IT Department share the findings of the assessment with the key users in LCB Finance and their comments, if appropriate, should be taken into consideration. Subsequent to the users' comments are incorporated, the IT Steering Committee should via the IT Department develop an IT Capability Current Status Assessment Report and send it to the Director Finance for review.

The Chairman should review the IT Capability Current Status Assessment Report. Once the Chairman reviews the IT Capability Current Status Assessment Report, the IT Steering Committee should use this report as a basis for the IT Strategic Planning process.

IT Strategic Plan

The IT Strategic Plan shall define how IT is to contribute to the achievement of LCB Finance's strategic goals and objectives. The IT Strategic Plan shall define how IT shall support IT Investment programs and operational service delivery. The IT Strategic Plan shall cover investment/operational budget, funding resources, sourcing strategy, acquisition strategy, and legal and regulatory requirements.

A portfolio of IT Operational Plans shall be derived from the IT Strategic Plan. Responsibilities for the execution of the operational plans shall be assigned appropriately and the expectations in terms of implementation, performance and outcome shall be clearly defined.

Associated Procedures

The IT Steering Committee should meet annually to devise the IT Strategic Plan that should be divided into a number of IT operational Plans. Additionally, the IT Steering Committee should confirm that the IT Strategic Plan is in total conformity with the legal/regulatory requirements relating to the IT Infrastructure.

Once operational plans are developed, the IT Steering Committee should approve budgets, key milestones and timeframes to all the IT Operational Plans. Also, the IT Steering Committee should approve responsibilities for the pursuit of the IT Operational Plans.

Accordingly, the IT Steering Committee should define critical success factors (CSFs) to monitor the success of each of the IT Operational Plan's implementation. Also, the IT Steering Committee should define key performance indicators (KPIs) to monitor the performance for each element of the IT Operational plan. The person(s) responsible for the IT Operational Plans should report their performance plans to the IT Steering Committee at each key milestone.

Upon defining CSF and KPI for each operational plan and overall for the IT Strategic Plan, a compiled IT Strategic plan inclusive of all operational plans and corresponding measures should be sent to the Director Finance for review.

The Director Finance should review and approve the IT Strategic plan and its operational plans along with budgets and implementation schedules.

Maintain and Update the IT Strategic Plan

The IT Strategic Plan shall be reviewed periodically (preferably; bi-annually) to ensure that new/changing business/IT requirements are addressed, and the IT Strategic Plan shall be updated accordingly.

Associated Procedure

The IT Steering Committee should monitor the progression of the IT Strategic Plan through the observation of the IT Operational Plans implementation based on the CSFs/KPIs identified in the IT Strategic Planning process.

In the case of any changes in the business/IT requirements of the entity, the IT Steering Committee should hold an immediate meeting to address those changes and update the IT Strategic Plan accordingly. All updates to the IT Strategic Plan should be compiled and sent to the Director Finance for review and approval.

Accordingly, the Chairman should review and approve the updates to the IT Strategic Plan and any budget requirement based on justifications provided for these updates.

Align IT Risk Management with Business Risk Management

An IT Risk Management Team shall be formed of the Chairman, HOIT, Managers representing LCB Finance and Department Heads. The IT Risk Management Team shall have a well-defined methodology to integrate the IT Governance, IT Risk Management and Control Frameworks with the overall Risk Management Framework.

The IT Risk Management Framework shall be in line with LCB Finance's risk appetite and risk tolerance.

Associated Procedures

The IT Risk Management Team should meet annually and as appropriate to review the Business Strategic Plan and identify any associated business risks. Based on the identified risks the IT Risk Management Team should set a defined and agreed upon risk appetite and risk tolerance levels.

Based on the identified risk appetite and tolerance levels, the IT Risk Management Team should establish criteria against which risks are evaluated. Those criteria should be rationalized by the respective Department Heads and business process owners and properly documented and sent to the Director Finance for approval.

Risk Assessment

The IT Risk Management Team shall identify any information resources and/or IT related products in LCB Finance. The IT Risk Management Team shall assess all the threat agents, threats, weaknesses and/or vulnerabilities with potential impact on all of the information resources, personnel and IT related products in LCB Finance.

The IT Risk Management Team shall determine the nature of the impacts identified and prioritize the risks associated with the impacts depending on their degree of effect on LCB Finance. The IT Risk Management Team shall coordinate with all the relevant process/data owners to identify appropriate controls by which risks are minimized or eliminated. The residual risks shall be agreed upon. They shall

create a register for documenting risks and exceptions. For each risk the following should be taken into consideration:

- Determine a risk score based on impact and likelihood
- Identify a risk owner
- Select an appropriate treatment
- Have senior management sign-off and the risk- and exception log yearly or in case of risks with great impact

The IT Risk Committee shall document and implement a security incident process describing the steps for registration, classification and handling. Include a description on how a root cause analysis is performed and have the process approved by the senior management.

Associated Procedures

The IT Risk Management Team should have an up-to-date inventory of all information resources and assets in LCB Finance which is an input from the asset management processes. For each information asset the IT Risk Management Team should prepare a list of all the identified possible risks, the associated processes, the business process owners, and should assess the likelihood and frequency of all the identified risks and their impact on LCB Finance and should properly document such information.

Once risk assessment results are compiled, the IT Risk Management Team should identify the appropriate response actions for all the identified risks, prepare a Prioritized Risk List depending on the likelihood and frequency of occurrence of each identified risk. The Prioritized Risk List should be sent to the Chairman for review and approval.

The Chairman should review and approve the Prioritized Risk List within 1 month. Once approved by the Chairman the IT Risk Management Team should proceed to Risk Management plan development.

Risk Management Plan

The IT Risk Management Team shall establish a Risk Management Plan. The Risk Management Plan shall be divided into plans of actions and projects to implement the agreed risk treatment plans. The implementation of the action plans and projects shall be monitored, and the progress shall be reported to the Chairman.

Associated Procedures

Based on the Prioritized Risk List the IT Risk Management Team should identify implementation responsibilities for each action plan or project. Corresponding critical success factors (CSFs) should be developed to monitor the success of each action plan or project and Key performance indicators (KPIs) should be developed to monitor the performance of each action plan or project.

Create a risk profile, based on in- and external factors that could have negative impact on the firm and determine how much risk the firm is willing and allowed to take (risk level or risk appetite). Have the risk profile signed-off by senior management and create a procedure for risk treatment containing at least:

- The way risk assessments are to be carried out (methodology)
- The calculation of risk (based om impact and likelihood)
- Treatment options
- Approval and reporting

Describe how the residual risk is determined after implementing mitigating controls and include the description the document mentioned above (Risk treatment procedure).

Create a template for risk treatment and fill out this template for each critical system or application identified. Once CSFs and KPIs are set, a monthly progress report of the action plans and projects and their performance measures should be developed by the IT Risk Management Team and provided to the Chairman.

Additionally, a quarterly progress report of the Risk Management Plan should be developed by IT Risk Management Team and provided to the Chairman.

The IT Risk Management Team should continuously identify new/changing risks and accordingly, should define appropriate controls to mitigate identified risks.

The IT Risk Management Team should meet quarterly at minimum or exceptionally when a critical risk is identified to ensure that the Risk Management plan is properly updated, and new/changing risks are identified, and appropriate controls and actions are defined.

FORMS/TEMPLATES TO BE USED/REFERED

- Risk Grid
- Risk Register

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- IT Strategic Plan
- Risk Assessment
- Change Management Policy
- Network Management & Firewall Policy

External References

- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department.

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or Director Finance , depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

2. CHANGE MANAGEMENT

PURPOSE

This publication seeks to assist organization by providing a document for Change Management ensuring that a consistent and trouble-free computing environment is in place to ensure a stable IT environment, while maintaining quality, availability, cost effectiveness and responsiveness and to establish procedure for deploying latest patches and updates on all the components of the network (hardware, software and services). All reasonable effort must be taken to ensure compliance with the procedure.

INTRODUCTION

The document applies to the IT Administrator and IT Support Team responsible for handling patch management of all Servers, Desktops and Network Devices in LCB Finance and includes maintaining an effective Change Management Framework for executing and monitoring the changes to infrastructure, application programs and configuration.

SCOPE

This SOP includes guidelines applies to the policy applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance regardless of the geographic location.

This Policy covers all Information Systems (IS) environments operated by the entity and/or contracted with a third party by LCB Finance.

All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her Systems Administrator, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy.

OBJECTIVES

- To ensure that the generic IT Service processes regarding Configuration, Incident-, Change-, and Problem management are in place
- To determine the adequacy of Performance and capacity monitoring and follow-up processes are in place for all business-critical systems and processes
- To ensure documented procedures are made available and accessible for all employees involved.
- To ensure that all systems and network components are identified and centrally registered before being elevated to production status in a Configuration Management Database (CMDB) or equivalent registration
- To determine whether procedures exist to keep the configuration database accurate and up to date.
- Create a procedure which ensures that all changes to production systems follow the change management process, for instance by implementing segregation of user rights (a person requesting something to be changed does not have sufficient administrative credentials to actually make the change)
- Embed Change management in the Patch management process.

- All systems and network components are identified and centrally registered before being elevated to production status in a Configuration Management Database (CMDB) or equivalent registration
- Procedures exist to keep the configuration database accurate and up-to-date.

DEFINITIONS

Change Management: This provides a systematic approach for raising any issues related to changes in the production environment. This ensures the Change Request being raised, assigned and resolved efficiently.

Change request: This document is required for any update, modification, and upgrade, addition, and deletion, replacement for hardware, and software, network and facilities environments on any component that affects production availability.

Patch Management is an important part of keeping the IT components of the network securely available to the end user.

Patch Management: Provides process of updating regularly the software, firmware and drivers. Patch Management should be a centralized, managed service that guarantees protection, rather than a user-installed approach that leaves the state of the network unknown.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any inquiries regarding this policy shall be directed to the IT Department.

Role	Designation	Responsibility
Process Owner	Head of IT	Section 07
Process delegates	IT Executive	

SPECIFIC PROCEDURE

LCB Finance shall ensure that all changes, including emergency maintenance and patches, relating to infrastructure and applications within the production, test environments must be formally managed in a controlled manner. Changes (including procedures, processes, and system and service parameters) shall be logged, assessed and authorized prior to implementation and reviewed against planned outcomes following implementation.

The entity shall ensure proper mitigation of the risks negatively impacting the stability or integrity of the production environment and ensure the establishment and maintenance of an accurate and complete configuration repository to maintain the integrity of hardware and software configurations.

a. **Change Standards and Procedures**

The Manager IT shall be responsible for setting up formal Change Management Procedures to handle all requests and/or requirements in a standardized manner (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

Change Management is the most critical component of LCB Finance and hence the below mentioned procedure must be followed to ensure confidentiality, integrity and availability of the system.

- All users accessing LCB Finance network and resources have to raise a Change Request for any issues related to any purchase, update, modification, upgrade, addition, and deletion, replacement for hardware, software, network and facilities environments on any component that affects production availability.

The Change Request form should be duly filled as discussed below:

1) **Contact Information:** <Contact details of the user requesting a change>

   Name: <Name of the user>
   Department :< Name of the department>
   Phone :< Phone no. of the user>
   Email: <Email id of the user>

2) **Change Request Details :<**Change Request details have to be filled by the user>

   Change Request No. :< This has to be referred from the LCB Finance Change Request Activities spreadsheet>
   Change Request Name :< The activity name has to mentioned as per the Change Request No. raised>
   Change Description :< Detailed description of the change required>

3) **Change Impact** :<Impact of the change have to be mentioned as this will help in deciding the criticality of the activity>

   Critical -<Changes that are required, unexpected and unplanned. Changes of type Critical should happen at any time during the weekday requiring immediate production change. Notification to users is immediate>
   High -<Changes that are required, unexpected and planned. Changes of type High should happen on any weekday during working hours. Notification to users is for more than 1 day >
   Medium -<Changes that are required, expected and planned. Changes of type Medium should happen on any weekday after working hours or on weekend. Notification to users is for more than 3 days>
   Low -<Changes that are required, expected and planned. Changes of type Low should happen only on weekends. Notification to users is for more than a week>
   Note: The change types - Medium and Low are referred as Normal change in most of the policy and procedure documents as they are expected and planned.

   a. **Number of Users Affected and Users Notified By:<**Any user raising the change request should clearly mention the number of users getting affected because of this change and how the users will be notified. Notification can happen either by mail or by phone in case of emergency>
   b. **Business Reason :<**Any user raising the change request should explain in detail the business justification for the requested change>
   c. **Schedule :<** The Change Request schedule is decided by the assigned person for this change. He/She should provide the scheduled date and window time for this change. He/She should provide the date and window time depending on the change type and number of users getting affected>
   d. **Back out procedure:<**This procedure should explain in detail the roll-back procedure in case it makes system instable after the change>
   e. **Resources Required:<**This should also mention whether they require another resource to help during the change>
   f. **Budget required:** Yes/ No <This should be mentioned only in case of purchase of any equipment or additional peripherals or modules>

g. **Assigned to** :<Name of the person who will work on this change>
h. **Tracking ID** :<This is number to be allocated by the IT Support Team for tracking of the change state whether it is open/assigned/closed>
i. **Status:** Approved/ Rejected <The status shows whether the Change Request is approved or rejected>
j. **Signature:** <This has to be signed by the authorized persons designated as 'Approvers' for the changes to be approved or rejected>
k. **The following are the Approvers and depending on the changes;** it should require approval from the respective Heads as discussed in the LCB Finance Security Policy and Procedures:
    - Human Resource Head
    - Department Head
    - Admin Head
    - IT Manager
    - Information Security Officer
    - Chairman
l. **Date:** <The date when the approvers approve the change request>

- The Change Request Form duly filled by the user should be sent to the respective support team by mail. The copy of the mail should be sent by the user to respective the Department Head for approval
- The Department Head should get the approval from the IT Admin depending on the change activity
- The IT Admin should get approval depending upon the criticality of the change from the Head of IT
- After the approval, the assigned person should execute the changes and send the mail to the requested user for verification and confirmation
- The user should verify and confirm that the changes that have been done as per the request. If the change has not been effective/ resolved, he/she should send the mail to the assigned person and ask him/her to reinvestigate and rectify the issue
- The assigned person should send the mail to the user for verification and confirmation. User should send the mail to the assigned person confirming the satisfaction with the resolution of the change request
- Assigned person for the Change Request should send the mail to the approvers of the Change Request confirming the resolution and marking the Change Request asCLOSED.

Associated Procedures

The IT Department should define and document procedures for information asset changes. Those procedures should be based upon agreed standards.

Once procedures are defined, the IT Department should define the levels of approvals based on the severity of the change and the expected costs for acceptable information asset changes. Accordingly, the IT Department should define a process to monitor the compulsory information asset changes that are required to be reported to the legal/regulatory authorities.

Additionally, the IT Department should define and implement a methodology that is to be strictly followed in the pursuit of any information asset change.

As such, all requests for any information asset change should be submitted to the IT Department. The change request should clearly define the boundaries of the change, the need for the change, the goal of the change and the expected business benefits.

Accordingly, the IT Department should initiate the change management process and carry outthe change from testing to final delivery to production

As such, the IT Department should ensure that all changes are strictly applied in a Test Environment. Upon successful testing, the IT Department should approve the transfer of the change to the Production Environment

b. Impact Assessment, Prioritization and Authorization

The IT Department shall ensure that all requests for change are assessed in a structured way for impacts on the operational system and its functionality.

Associated Procedures

All change requests should, as previously mentioned, be submitted to the IT Department to assess the impact of the proposed changes on the IT Infrastructure, and collectively at LCB Finance operations, in terms of, but not limited to:

- The change category
- Cost Vs. benefit
- Importance
- Effort estimate
- Resources required
- Compliance with Change Management Policy
- Complexity
- Approval from the relevant business line head
- Conformity with current IT Infrastructure

Once the assessment is done, the IT Department should then define categories for all information asset changes. The categories should be formalized based on the changes' effect on the entity's IT Infrastructure and the potential benefits realized from the changes.

Based on the previous assessment and the categorization, the IT Department should then prioritize all changes requested. The IT Department should then prepare a "Prioritized Change List" and should then conduct a meeting to further investigate the Prioritized Change List and decide on the acceptance or denial of the changes.

The IT Department should then authorize all the accepted changes and develop Change Implementation Plans for the authorized changes. All the plans should be formally approved and documented by the Information Security Steering Committee.

Once change implementation plan is approved, the IT Department should develop a "Change Implementation Schedule" that contains the milestones for the execution of all the Change Implementation Plans as and when required. The Change Implementation Schedule should clearly assign responsibilities for the implementation of the plans.

The IT Department should define critical success factors (CSFs) to measure the success of the Change Implementation Plans as and when required.

In addition, the IT Department should develop key performance indicator (KPIs) to monitor the performance of the Change Implementation Plans. The responsible person for the implementation of each plan should provide performance reports on each of his/her plan's implementation milestones as and when required.

c. Emergency Changes

The Manager IT shall establish a process for defining, raising, assessing and authorizing emergency changes that do not follow the established formal change management process.

The Manager IT shall establish an efficient mechanism to handle emergency changes. The mechanism shall allow for timely implementation of such changes. The mechanism must ensure that documentation and testing shall always be performed.

Associated Procedures

Unless highly required for the continuity of critical business operations, the IT Department should ensure that all the emergency changes are applied and tested in a Test Environment. Subsequent to the implementation of the emergency change, the IT Department should prepare a detailed documentation of changes performed as and when required.

Once the emergency situation is contained, the IT Department should review emergency changes and decide whether, or not, to leave the changes as permanent changes or to apply additional modifications/enhancements to the changes as and when required.

d. Change Status Tracking and Reporting

The Manager IT shall establish a tracking and reporting system for keeping change requestors and relevant stakeholders up to date about the status of the change to applications, procedures, processes, system and service parameters, and the underlying platforms.

Associated Procedures

The IT Department should implement and maintain a "Change Track Records List" to record all information asset change requests and changes performed for the entity's information assets.

Consequently, The IT Department should ensure that the Change Track Records List relate the changes to their relevant stakeholders, applications, procedures, processes, systems services parameters, and the underlying platforms they were applied for.

Upon collecting such information, the IT Department should report to the user of any important user actions, status reports and relevant event history as required. The change database is a valuable information asset and proper backup and protection to its data should be considered.

The change owner should ensure that all the documentation of the changes are completed after the implementation.

e. Change Closure and Documentation

The Manager IT shall ensure that updates to the associated system and user documentation and procedures occur whenever system changes are implemented.

Associated Procedures

The IT Department should ensure that all the documentation of the changes are completed after the implementation prior to closure. Upon aggregating all change documentations, the IT Department should ensure that the Change Track Records List is updated accordingly and that the completed/implemented changes are signed off with a closure notification

f. Configuration Repository, Baseline and Maintenance

- The Manager IT shall establish a central repository to contain all relevant information on configuration items.
- The Manager IT shall establish a well-defined methodology to identify and maintain configurations items.

- The Manager IT shall ensure that a baseline of configuration items is kept for every system and service as a checkpoint to which to return to after changes rollback.
- The Manager IT shall ensure that the procedures for identifying and maintaining configurations items shall provide proper authorization and logging of all actions on the configuration repository and be properly integrated with change management and problem management procedures.

Associated Procedures

The IT Department should ensure that the central repository includes hardware, application software, middleware, parameters, documentation, procedures and tools for operating, accessing and using the systems and services. Relevant information to consider are naming, version numbers and licensing details.

Once all of the relevant information assets are identified, the Configuration item details should be updated in the repository upon completion of the configuration process. Accordingly, the configuration repository should be compared with each change request to provide feedback and quick fix actions

g. Configuration Integrity Review

- The Manager IT shall ensure the integrity of the configuration data by periodically reconciling the current configuration state with the documented records.
- The Manager IT shall ensure that errors and deviations are reported, acted upon and corrected in a timely manner.

Associated Procedures

The IT Department should reconcile the configuration repository quarterly and as and when required. Accordingly, all identified updates based on the reconciliation should be properly documented and reflected in the repository Additionally, all employees should report errors and deviations to the IT Department that should act upon and accordingly follow the change management processes. The IT Department should ensure timely follow-up and closure of open calls and follow proper escalation paths.

h. Patch Management Procedure

i. Audit Current State

The current state of the network should be understood clearly by the IT Team before we can maintain the network. This involves identifying:

- Hardware
- Software
- Operating systems, applications, database and their patch levels
- Other hardware and peripherals such as printers, switches, servers and network devices that have firmware

Once the current state of the network is known, IT Support Team should plan to bring it up to date by installing the latest drivers, patches, firmware and definitions. A baseline should be created from where regular patch maintenance can be done.

ii. Security and Patch Information Sources

- IT Admin should facilitate to get updates about the timely release and distribution of information on product security issues and patches on their key operating system, database, network device and application from vendors.
- This should also include monthly calls with the account manager and simple subscriptions to the vendor's security announcement list
- Use of Patch Management Software may be advised for automatic download of latest security patches and service packs for Operating systems, applications, software's and database. The IT Admin should make available a list or spreadsheet of manufacturer's websites that hold the patches and updates in the configuration management database to give all IT Support Team access to this important information.

iii. Patch Deployment

New Patch Availability

- New Patch availability from various sources as per section 5.2 will usually have some release information explaining what the patch fixes and who should use it. IT Administrator should read this information carefully and ensure that the patch applies to the components and overall network structure of LCB Finance. The patch may not be applicable to every component on the network, in which case he/she should need to identify which components require the patch
- Most of the patches are provided with the ratings. These ratings are defined by the vendor depending on the criticality of the patches or updates. Few Patches or updates may come with critical rating and hence IT Administrator should deploy such patches by evaluating an impact analysis. If the impact is critical, he/she should ensure the deployment of such patches immediately through Change Management.

Acquire Patches

- Patches may be acquired either by downloading it from the internet, getting it sent by post (CD's, DVD etc.), patch management software or having it emailed to the IT Administrator.
- Few service packs or new versions that are hundreds of megabytes in size may be requested on CD to save bandwidth and download time.

Test Patches

- Patches should be tested on servers or desktops or other devices that are reserved for testing. The testing itself depends on what the patch claims to fix
- Once the IT Administrator is satisfied that the servers or desktops or other devices still works properly and that the patch has not created other issues, proceed to the next phase
- If critical patches are to be installed, it should be tested immediately as this should have higher priority than other patches that can be tested and installed phase wise.

Deploy Patches

- IT Administrator should raise a Change Request for the installation of patches with a detailed business reason for justification.
- The Change Request should also include the Back-out procedure in case the patch installation creates system instability.
- The Change Request should be assigned to the IT Support Team and a mail should be sent to the Chairman for approval.
- If the Change Request is critical, it should be scheduled, to be installed immediately after Chairman approves the Change Request. The IT Support Team should install the patch and send the mail to the Chairman.

- The system should be reviewed for few hours and verified whether all the applications and database are working fine.
- If the system is unstable the Back-out procedure should be initiated to bring the system back to the previous state and all applications and database should be verified to ensure stability
- The same process should be followed if the Change Request is Normal except that the patch should be deployed on weekends after Chairman approval
- After the successful installation and verification of the patches on the system, IT Support Team should mark the ticket as CLOSED and confirm by sending mail to the IT Administrator and IT Manager.

FORMS/TEMPLATES TO BE USED/REFERED

- Change Management Form

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Incident Management Policies
- IT Asset Management Policy
- Network Management & Firewall Policy

External References

- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department. Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department.

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or Director Finance , depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

3. INCIDENT AND VULNERABILITY MANAGEMENT

PURPOSE

This publication seeks to assist organization in mitigating the risks from IT infrastructure incidents by providing practical guidelines on responding to incidents effectively and efficiently. The purpose of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, ensuring that agreed levels of service quality are maintained.

INTRODUCTION

The IT resources at LCB Finance support the operational and administrative activities of the organization. The SOP is designed to minimize the system downtime and to protect the system against broad range of threats including hackers, viruses and malware.

IT incident management is an area of IT service management (ITSM) wherein the IT team returns a service to normal as quickly as possible after a disruption. An incident is an unexpected event that disrupts the normal operation of an IT service.

SCOPE

SOP includes guidelines on establishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing and handling incidents. Security malfunctions and service requests (requiring access, connectivity, restoring of backups, functionalities, etc) are registered in a centrally managed system and assigned a unique ID.

OBJECTIVES

- Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents.
- Increase visibility and communication of incidents to business and IT support staff.
- Security related malfunctions and service requests (requiring access, connectivity, restoring of backups, functionalities, etc) are registered in a centrally managed system and assigned a unique ID
- Tickets/requests are routed to the appropriate solver- or authorization group
- All actions shall be logged under the original and unique ticket number.
- A documented procedure is in place to investigate the root cause of major incidents and control the restoring of functionality of all (reoccurring or) high impact incidents.
- Known issues and fixes are documented.
- Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur
- Align Incident Management activities and priorities with those of the business
- Maintain user satisfaction with the quality of IT services

DEFINITIONS

Service Level Agreement: A service-level agreement (A) is a commitment between a service provider and a client. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service use.

Annual Maintenance Agreement: An annual maintenance contract (AMC) is an agreement with a service provider for repair and maintenance of property used by your company. Typically, AMCs include service support; however, you can add a comprehensive maintenance contract (CMC) that will cover IT support and replacement as well.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	IT Executive

SPECIFIC PROCEDURE

LCB Finance should develop, communicate and implement formal systems and procedures for detecting, reporting, and investigating incidents relating to exceptional situations in day-to-day administration and operations of IT and information security related areas.

It should be ensured that incidents are reported on time to the appropriate authorities and corrective action is taken immediately to avoid the recurrence of such events.

All staff, contractors, and other users of LCB Finance's information are responsible for helping to ensure the security of the computer systems that they use and operate. Part of this responsibility is the duty to report confirmed or suspected security problems in a timely manner to the appropriate authority.

Incident identification

A security incident could be defined as the act of violating the security policy. The following is an illustrative list of what actions can be classified as incidents.

- Attempts to gain unauthorized access to a system or its data, masquerading, spoofing as authorized users.
- Unwanted disruption or denial of service.
- Unauthorized use of a system for the processing, transmitting or storing of data by authorized/ unauthorized users.
- Changes to system hardware, firmware or software characteristics and data without the knowledge of application owner,
- Existence of unknown user accounts and/or
- Unauthorized disclosure of company information
- Appropriate detective mechanisms need to be designed for timely detection of information security incidents.
- Preventive controls must be put in place to minimize the occurrence of information security incidents.
- All information security incidents require to be recorded as per the information security incident management process.
- Appropriate forensic methods need to be applied, whenever required, to collect evidence in the course of investigation of information security incidents. This must be done by a trained forensics investigator.

Incident response team

LCB Finance must organize and maintain an Incident Response Team (IRT) that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related security incidents such as virus infestation, and miscellaneous intrusions.

The incident response team members have predefined roles and responsibilities assigned as per the

incident management policy, which may take priority over their normal duties during critical incidents.

To ensure a quick, effective, and orderly response to incidents, the incident response team will define procedures for handling incidents.

Incident reporting

Immediately upon identification, all IT incidents whether confirmed or suspected, must be reported to LCB Finance IT department through appropriate management channels as quickly as possible.

All employees and third-party users of LCB Finance information assets need to be informed and need to be aware of the incident reporting procedures, prior to granting access rights to LCB Finance information resources.

It is required that all employees, contractors and third parties report all suspicious activity, and necessary steps must be taken to protect the privacy and confidentiality of any party providing such information.

Confidentiality of incidents

Any employee, upon identifying incidents, must not disclose any information regarding the incident other than as per the instructions provided by the incident response team as incidents could lead to serious financial or reputational damage to LCB Finance when publicized. **Hence all IT related incidents must be considered as confidential information.**

Only the LCB Finance Management or a person appointed by the Management team has the authority to disclose any incident to the public or other external parties.

Incident investigation

All reported incidents must be logged and classified according to specific criteria relating to the criticality of the incident as specified by LCB Finance.

Incident response procedures require including specific procedures to discover, protect, record, collect, identify and preserve evidence related to the incident in a manner that will not render it unacceptable in a court of law.

LCB Finance will investigate incidents based on established criteria as relevant to the security incident.

Documentation and analysis of incidents

LCB Finance should learn from all identified/materialized incidents and develop procedures to analyze each security incident to identify root causes, damage/cost of incident, and strategies in order to prevent similar incidents occurring in the future and to minimize the impact of similar future incidents.

LCB Finance IT must maintain complete documentation regarding each security incident.

Incident reporting and Monitoring

Upon identifying IT incident (e.g., virus infection, system outage, hack-in attempts), regardless of whether realized or suspected, immediately inform the IT Department via phone and e-mail. If informed via phone the Support person from IT Department should complete the IT Incident report with required details to proceed. If incident is reported in writing, IT incident report form must be used by the reporting person.

Carry out the instructions provided by the IT Department to address the issue or to obtain further information.

Fill in the Incident Reporting form (Annexure C) and submit it to the IT Department. Once an incident has been notified and if the incident needs to be alerted to customers, counter parts and any other stakeholders who can be affected by this incident, this must be informed to them by the LCB Finance Management Team or someone appointed by the Management team.

Once the incident is reported, IT Department should ensure that the incident has been logged.

Incident Response Team should evaluate the criticality of the incident and take necessary action to prevent further damage.

The evidence collected as part of the analysis should be safely stored. This evidence should be used if the incident warrants civil or criminal action against organization or personnel.

Follow up and obtain the Incident Reporting form from the user who reported the incident.

Complete the incident report, with action steps and decisions made. Once the Incident is closed, submit a copy of the incident form to the Head of IT.

The IT incident management lifecycle

- Incident logging.
- Incident categorization.
- Incident prioritization.
- Incident assignment.
- Task creation and management.
- LCB Finance management and escalation.
- Incident resolution.
- Incident closure.

3.1.1.1. Incident logging

An incident can be logged through phone calls or emails. IT department issue the IT Incident Report Form. User need to fill the required details of form and user need to sign the form.

3.1.1.2. Incident categorization

Manager/ IT executive will check the incident properly and they need to give comment about the incident. Incidents can be categorized based on the area of IT or business that the incident causes a disruption in like network, hardware, software, security etc.

3.1.1.3. Incident prioritization

The priority of an incident can be determined as a function of its impact and urgency using a priority. The impact of an incident denotes the degree of damage the issue will cause to the user or business. The urgency of an incident indicates the time within which the incident should be resolved. Based on the priority, incidents can be categorized as:

- Critical
- High
- Medium

- Low
- After approving the ticket by Head of IT details is entered into excel file.

3.1.1.4. Incident assignment

Once the incident is categorized and prioritized, it gets routed to an IT executive with the relevant expertise. He will start the rectifying issue.

3.1.1.5. Task creation and management

Based on the complexity of the incident, it can be broken down into sub-activities or tasks. Tasks are typically created when an incident resolution requires the contribution of multiple technicians. When parts need to order for hardware equipment, IT executive need to get approval from Head of IT and CEO. If hardware items (desktop, laptop, printer, UPS etc). need to send out of premises, IT executive need to send list of items to the Manager IT via e-mail. As well as he needs to fill IT equipment in and out records book and get the approval from Head of IT and or CEO.

Head of IT/ Executive IT will coordinate with vendors who signed A with LCB Finance, if IT department need to assign to job them related hardware, software, network and security incident. Job card is needed to get from vendors when the IT equipment is handed over.

Meanwhile Manager -IT need to escalated problem to Administration department if there is any insurance claim related incident. After collecting the claim, it needs to enter excel file of insurance claim. Incident details is needed to enter in manual register.

If IT equipment is to be discarded, the relevant discarding procedure needs to be followed.

3.1.1.6. A management and escalation

While the incident is being processed, the IT executive needs to ensure the A isn't breached. An A is the acceptable time within which an incident needs response (response A) or resolution (resolution A). In cases where an A is about to be breached or has already been breached, the incident can be escalated functionally or hierarchically to ensure that it is resolved at the earliest.

3.1.1.7. Incident resolution

An incident is considered resolved when the technician has come up with a temporary workaround or a permanent solution for the issue.

3.1.1.8. Incident closure

An incident can be closed once the issue is resolved and the user acknowledges the resolution and is satisfied with it. If incident is resolved, ticket is needing to sign off with signature of head of IT.

FORMS/TEMPLATES TO BE USED/REFERED

- IT Incident Report

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Network Management Policy
- Change Management Policy

- Business Continuity Plan
- Disaster Recovery Plan

External References

- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or Director Finance , depending on the criticality. The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

4. DATA CLASSIFICATION POLICY

INTRODUCTION

Information Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by company law as well as proprietary, ethical, operational, and privacy considerations. All company data, whether electronic or printed, should be classified.

The data owner, who is responsible for Data Classification, should consult with legal counsel on the classification of data as Confidential, Internal, or Public. Consistent use of data classification reinforces with users the expected level of protection of company data assets in accordance with company security policies.

SCOPE OF POLICY

Any employee, temporary worker, contractor, third-party user that uses and have access to company information network remotely or directly must comply with the policy stated below. Any electronic tool that is owned, developed and managed by the company is also subjected to this policy.

This policy should be adhered to whenever using company information in any format directly or indirectly, and by any means.

Company data created, sent, printed, received, or stored on systems owned, leased, administered, or authorized by LCB Finance PLC are the property of LCB Finance and its protection is the responsibility of the respective owners, designated custodians, and users. Access control rules and procedures are required to regulate who can access company information resources or systems and the associated access privileges.

POLICY STATEMENTS

It is the policy of LCB Finance that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle.

This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 4 (four) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity within LCB Finance PLC.

At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy.

All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

All involved systems and information are assets expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

The proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system. Data used for authentication shall be protected from unauthorized access. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to Certis systems and their resources. Remote access shall be controlled through identification and authentication mechanisms.

All users who come into contact with sensitive internal information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily business activities.

Storage media containing sensitive information shall be completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased it must be destroyed in a manner approved by the Head of IT Department.

If restricted information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must conform to data access control safeguards approved by this policy and company management. When these users are not currently accessing or otherwise actively using the restricted information on such a machine, they must not leave the machine without logging off, invoking a password protected screen saver, or otherwise restricting access to the restricted information.

Files containing confidential or sensitive data may not be stored in PCDs (Personnel Communication Device) unless protected by approved encryption. Confidential or sensitive data shall never be stored on a personal PCD. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-by-case basis.

The cost of any item beyond the standard authorized equipment is also the responsibility of the employee. Lost or stolen equipment must immediately be reported.

CLASSIFICATION OF DATA

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

Confidential

Confidential Information is very important and highly sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.
Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law or company policy, and other constitutional, statutory, judicial, and legal agreements.

Internal / Official

Internal / Official information is intended for unrestricted use within the entity, and in some cases within business partners of LCB Finance. This type of information is already widely-distributed within LCB Finance PLC, or it could be so distributed within the organization without advancepermission from the information owner. Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.
Any information not explicitly classified as Confidential or Public will, by default, be classified as Internal Information.

Public

Public Information has been specifically approved for public release by a designated authority within LCB Finance PLC. Examples of Public Information may include marketing brochures and material posted to internet web pages based on the Right to Information Act No.12 of 2016 and other legislative requirements.

COMPLIANCE

If any user is found to have breached this policy, they may be subject to company's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

5. IT ASSET MANAGEMENT

PURPOSE

The purpose of this policy is to help LCB Finance for create and maintain an Asset Management Framework.

INTRODUCTION

The Asset Management Policy describes the aims and objectives of IT asset management. This policy draws from IT industry best practice using the ITIL framework, Controls Objectives in IT (COBIT 5). This asset management policy provides the framework for the care and control of IT assets through their life cycle. The 5 life cycle phases cover acquisition, deployment, operation and maintenance through to decommissioning (retirement) and disposal of assets.

SCOPE

This SOP covers how the Asset Management Policy is to define a coherent set of principles, policy statements, processes, standards and architectures that

- Describe how IT assets are managed
- Provide high level policy statements on the requirements for managing assets
- Identify key standards, processes and procedures which support the policy
- Define the roles and responsibilities for implementing this policy
- Define technical solutions that support the delivery of the asset management policy.

It applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance regardless of the geographic location.

OBJECTIVES

The objectives of this policy is to,

- Maintain control over physical IT assets purchased and owned by the LCB Finance
- Provide accurate IT asset information for the annual financial statements of the LCB Finance which is required for accrual reporting purposes
- Allow audit verification of additions to and deletions from the asset register
- Ensure compliance with LCB Finance's IT Security Policies in respect of IT asset management and any other legal obligations.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	IT Executive
	HODs

SPECIFIC PROCEDURE

4.6.1. Responsibility of IT Assets

- The IT Department shall clearly identify all Information assets.
- The IT Department shall draw up and periodically update an inventory of all Information assets.
- The IT Department in coordination with Business Departments shall assign an "Owner" (a person or a part of LCB Finance) to each asset associated with information processing facilities.
- The IT Department in coordination with Business Departments shall identify, document and implement rules for the acceptable use of asset associated with information processing facilities.

Associated Procedures

The IT Department should conduct an annual inventory of all information processing assets at LCB Finance. Once a complete list of information assets is finalized, the IT Department should assign all the information assets to Owners and an Asset Owner register should be developed and documented From there onwards, the IT Department is responsible for quarterly and requirement based updating of the Asset-Owner register and should integrate the change management process to identify and reflect any changes in asset ownership assignments

IT Assets and Information Classification

LCB Finance shall define classification criteria for all information assets.

Associated Procedures

The IT Department should establish the classification of IT assets criteria in terms of the assets: Value Legal requirements Sensitivity and criticality to LCB Finance. Once the criteria information is obtained for each IT assets, the IT Department should classify all IT assets in LCB Finance under the defined classification criteria.

4.6.3. IT Assets Maintenance

All valuable hardware assets (IT equipment, air conditioners, UPS etc.) should be labelled, recorded on IT asset inventory and maintained. Any material moving in and out of the office should be recorded in a register by the security. All such materials should be checked thoroughly by the security and should be informed to the admin department. Separate registers have to be maintained for returnable and non-returnable IT equipment.

4.6.4. IT Assets Performance and Capacity

- LCB Finance shall ensure that a formal periodic monitoring and review process exists to monitor the performance of important Information assets.
- The IT Department shall conduct periodic training sessions for LCB Finance Business Users of the IT assets to ensure acceptable use and performance.
- The IT Department in coordination with Business Departments shall estimate future
- Information assets' requirements based on capacity and availability requirements.

Associated Procedures

The IT Department in coordination with information asset owners should develop KPIs for each information asset that should be used to perform a periodic review of the performance of all information assets Based on the identified KPIs and the measurement data collected for these KPIs the IT Department in coordination with information asset owners should reassess the KPI acceptable level based on business future required operating levels According to the identified required performance levels, the IT Department should assess all information assets in order to develop a list of all the assets that need special or general training For the information assets that require general training, periodic training sessions should be conducted to users of those assets and continual measurement of KPIs should indicate the effectiveness of provided sessions For the information assets that require special training, the IT Department should contact the vendors or expert organizations to conduct special training sessions for the users of those assets Additionally, the IT Department should bi-annually conduct meetings with each Business Department to estimate the department's future information assets requirements. The forecast should be based on the capacity and Availability of the asset.

4.6.5. IT Equipment Maintenance or Repair at Off-site Premises

- Equipment under warranty should be taken to off-site premises for maintenance
- or replacement or repair and handled securely by the contracted third party/ vendor
- Equipment containing storage media should be checked to ensure that sensitive data and licensed software has been removed prior taken to off-site premises.
- Equipment taken off-premises should be authorized by Head of IT with appropriate business reasons and logged in the asset inventory
- Equipment taken off-premises for maintenance/ repair/ replacement should be
- logged in the returnable or non-returnable IT assets register maintained by IT department.

4.6.6. Return of IT Assets

All employees, contractors and third parties should return LCB Finance SRI LANKs information and physical assets in their possession upon termination of the employment relationship or contract.

This should include,

- A formal process for return of LCB Finance's hardware, software and data media should be enforced
- A formal process for return or destruction of organizational data of any kind should be enforced where the employee, contractor or third party uses personal equipment, requirements for secure erasure of software and data belonging to the organization should be done.

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy

- Change Management Procedures
- Incident Management Procedures
- User Management Procedure

External References

- ISO 27000

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT and/or Director Finance , depending on the criticality. The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

6. IT SECURITY TRAININGS AND AWARENESS

PURPOSE

The purpose of this document is to help LCB Finance. Ensure that employees make effective use of Information Technology assets in compliance with Security Policy and there exists a comprehensive training and development plan to help train employees on security issues.

INTRODUCTION

Establishing and maintaining information-security awareness through a security awareness program is vital to a LCB Finance's progress and success. A robust and properly implemented security awareness program assists the organization with the education, monitoring, and ongoing maintenance of security awareness within the organization.

A successful security awareness program within an organization may include assembling a security awareness team, role-based security awareness, metrics, appropriate training content, and communication of security awareness within the organization.

SCOPE

This policy applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance. Regardless of the geographic location.

This Policy covers all Information Systems (IS) environments operated by LCB Finance. And/or contracted with a third party by LCB Finance.

All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with IT department for clarifications. The IT Department shall assist resolve any conflicts arising from this Policy.

The Training and Awareness Policy covers:

- Security Awareness
- Users security education and training

OBJECTIVES

- To implement and asses appropriate ongoing awareness education and training, and regular updates in organizational policies and procedures for all employees, as relevant for their job function are in place.
- Implement procedures to periodically assess the current level of security awareness of all employees, by phishing tests or security awareness tests.
- Provide additional security training for employees working with business-critical systems and applications.
- Implement procedures to facilitate, record and measure periodic training activities to increase security knowledge of key users about high risk syste

DEFINITIONS

Security awareness (SA): It is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization

Phishing: Cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

RESPONSIBILITIES

Role	Designation
Process owner	Head of IT
Process delegates	Executive -IT

SPECIFIC PROCEDURE

Security Awareness

6.1.1.1. Periodic Awareness Sessions

The IT Department in coordination with the Human Resources and Administration Department and all other departments shall ensure that all employees of LCB Finance. Undergo continuous Security Awareness Program and periodic security awareness sessions to guarantee an acceptable level of security adherence in accordance with LCB Finance's Security Policy.

Associated Procedures

The Head of Information Technology in coordination with all other Department Heads should ensure an ongoing Security Awareness Program is executed weekly employing a variety of media. (E.g. posters, emails, company bulletin board, etc.)Proper tracking of each employee awareness coverage should be maintained by both the user department, the IT Department and the Human Resource and Administration Department Based on the awareness coverage information, the IT Department in coordination with the user department should schedule additional sessions to provide proper awareness on non-covered areas Accordingly, all assigned employees should attend as scheduled by their departments. Absence should be noted and justified as part of awareness, all Department Heads should encourage their employees to report any security breach incidents to their respective superiors through different communications means.

Educate and Train Users

6.1.1.2. Identification of Education and Training Needs

The Human Resources and Administration Department in coordination with the IT Department shall establish and periodically (bi-annually) update a curriculum for each target group of employees considering:

- Current and future business security needs and strategy
- Corporate values (ethical values, control and security culture, etc.)
- Implementation of new IT infrastructure and software (packages and applications)
- Current skills, competence profiles and certification and/or credentialing needs Delivery methods (e.g., classroom, web-based), target group size, accessibility and timing

Associated Procedures

The Human Resources and Administration Department in coordination with the Head of Information Technology should, based on the aspects mentioned above, formulate a Security Training Curriculum depending on the availability of courses and trainers whether internal (e.g. Head Of Information

Technology) or external consultant/entity. In case the training provider is an external consultant/entity, The Human Resources and Administration Department in coordination with the Head of Information Technology should contact that provider to check for the timeframe and available schedule for such provider additionally, there should be coordination with user departments to develop relevant schedules to allow adequate number of employee attendance.

The Human Resources and Administration Department and the Head of Information Technology should ensure that the time lag between the identification of training and the pursuit of it do not exceed 3 months Once, schedules are developed and finalized they should be communicated to employees attending the training and as applicable additional nominees should be assigned.

Delivery of Training and Education

- Based on the identified education and training needs, identify target groups and their members, efficient delivery mechanisms, teachers, trainers and mentors.
- Appoint trainers and organize training sessions on a timely basis.
- Registration (including prerequisites), attendance and performance evaluations shall be recorded.

Associated Procedures

The Head of Information Technology in coordination with all other departments should carry out periodic (Quarterly) General Security Awareness Sessions where the Head of Information Technology, an assigned person or a third-party expert person/entity hold a series of lectures meant to enhance the security mind-set of all LCB Finance's employees. Additionally, user departments should identify any training requirements and communicate this information to the Human Resources and Administration Department Accordingly, the Head of Information Technology in coordination with the Human Resources and Administration Department should, based on the identified education and training needs, identify target groups to receive relevant security training Once target groups are identified, the Human Resources and Administration Department in coordination with the Head of Information Technology should develop a "Training Schedule" based on the identified groups and the requirements and availability of trainers In case the training is dependent on prerequisites, the Human Resources and Administration Department should timely and efficiently notify concerned employees with those prerequisites and the specific schedule for them.

Registration for the training sessions should be easy and timely. Identified groups' employees should be encouraged by their Department Heads to participate for the sessions During training, the Human Resources and Administration Department should record attendance to the sessions and the attendance of employees should be investigated.

Employees should understand the Importance of attending such security training sessions and penalties/disciplinary actions should be clearly defined for absenting employees at the end of each session, the Human Resources and Administration Department in coordination with the Head of Security Department – as well as the training provider if possible - should prepare performance evaluation for each session.

Evaluation of Training Received

The IT Department and the Human Resources and Administration Department shall evaluate education and training content delivery upon completion for relevance, quality, effectiveness, capturing and retention of knowledge, cost and value. The results of this evaluation shall serve as input for future curriculum definition and training sessions.

Associated Procedures

The Human Resources and Administration Department should set key goal indicators (KGIs) such as, but not limited to:

- The number of training registration requests
- The percentage of employees trained

Those KGIs are to measure the degree to which the training program has achieved its intended goals and perform as input to future security training planning. Additionally, The IT Department should assess the effectiveness of the content delivered during the awareness sessions in terms of relevance to LCB Finance practices, coverage to important aspects of LCB Finance. Security needs, practicality and applicability of suggested course of actions.

Accordingly, the IT Department should utilize quiz assisted awareness to measure learning levels of each part of the awareness program and results should be evaluated to identify areas of deficiency in delivery.

These could include but not limited to:

- Insufficient or not relevant content
- Trainer is not qualified or not able to communicate the knowledge area to employees
- Lack of employees basic and prerequisite security knowledge
- Training environment is not proper, etc.

Once areas of deficiency and their associated causes are identified, the Human resource and Administration Department in coordination with the Manager IT should plan and execute proper remediation actions based on each cause.

FORMS/TEMPLATES TO BE USED

Compliance Declaration
Training Schedule
Acceptable Usage Policy

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Induction Booklet

External References

- ISO / IEC 27001-(1/2)

COMPLIANCE

Compliance with this Policy is mandatory. LCB Finance's Head of Information Technology must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by The IT Department and the Internal Audit Department.

Violations of the policies, standards, and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment
- Other actions as deemed appropriate by management, Human Resources, and the Legal Department

EXCEPTIONS

This Policy is intended to address Training and Awareness requirements. Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or Director, depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months). At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

The waiver shall be monitored to ensure its concurrence with the specified period for any exceptions.

All exceptions to this policy must be communicated through the Policy Waiver Request Form.

7. MALWARE PROTECTION & ANTI-VIRUS MANAGEMENT

PURPOSE

LCB Finance operates a technology environment that is essential for the continued business operation of firms and as such must be protected from a broad range of threats including hackers, viruses and malware.

As a result, LCB Finance implements this publication and technical controls for end point devices (computers, laptops etc.) and servers to mitigate associated risks including:

- Information systems be compromised by unknown parties.
- Information being corrupted, lost or destroyed.
- System performance being disrupted and/or degraded.
- Productivity losses being incurred.
- Failure to comply with regulatory requirements.
- Exposure to reputational risk.

INTRODUCTION

The increased growth and dependence on IT systems necessitates in appropriate support, security and contingency arrangements being in place to ensure system reliability and availability. One of the greatest risks to system stability and data integrity has been the growth in number and prevalence of malware software.

SCOPE

This SOP applies to all servers, computers, laptops etc. that are connected to the LCB Finance network via a standard network connection, wireless connection., modem connection, or virtual private network connection. Kaspersky end point security is installed for PCs as the malware protection.

OBJECTIVES

- To ensure all servers have malware protection solution installed and running.
- To determine that malware protection on servers is centrally managed.
- Forced software updates are applied to all devices as soon as new releases are available within an acceptable timeframe, but at least on a monthly basis.
- Real-time scans of active content are in place and scans of servers are configured on a weekly basis (as a minimum).
- Externally uploaded data to LCB Finance file sharing services is scanned for malware before it is internally distributed.
- All end-user devices are equipped with vendor supported malware protection, including but not limited to virus, spam and spyware.
- Forced malware protection updates are applied to all end-user devices daily.
- Real-time scanning of active content on end-user devices is configured weekly.
- Malware protection on end-user devices is centrally managed.
- To protect from virus, worm, spyware, phishing attacks, malware and other types of malicious software.

DEFINITIONS

Antivirus software: Antivirus software is known as anti-malware, is a computer program used to prevent, detect, and remove malware.

Virus: A computer virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. The virus requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator.

Worms: A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

Spyware: Spyware is software that aims to gather information about a person or organization, sometimes without their knowledge, that may send such information to another entity.

Malware: Malware, or malicious software, is any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of different functions such as stealing, encrypting or deleting sensitive data.

Phishing: Cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Executive IT

SPECIFIC PROCEDURE

Virus/Malicious Code such as network worms, Trojan horses, and logic bombs are unauthorized programs that replicate themselves and spread to other computer systems across a network. The symptoms of Virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.

Due to the mentioned reasons, LCB Finance shall have well-defined mechanism to prevent, detect Virus/Malicious Code and resolve the infected systems in a proper and timely manner.

Prevention of Virus/Malicious Code from Affecting Information Systems.

A Virus/Malicious Code Contingency steps shall be developed to define procedures and responsibilities to deal with and recover from Virus/Malicious Code attacks. All devices (LCB Finance and non-LCB Finance owned) shall be scanned for Viruses/Malicious Code prior to being connected to LCB Finance information assets.

All possible and practical measures shall be taken to prevent the introduction of Virus/Malicious Code into LCB Finance's information systems and network. Measures against Virus/Malicious Code would include but are not limited to the following:

Virus/Malicious Code prevention, detection and repair infrastructure shall be implemented at points where Virus/Malicious Code can be introduced into network.

A process to update the Virus/Malicious Code detection infrastructure with the latest product and Virus signature updates as soon as these updates are released shall be implemented.

The installation of Virus/Malicious Code protection software on any new potential point of entry (new PC's, servers, electronic mail, internet etc.) of Virus/Malicious Code or to determine that the new (potential) point of entry is covered by an existing installation of such software. The steps/decisions to be taken to protect LCB Finance's Information System infrastructure from a new Virus/Malicious Code - before LCB Finance's Virus/Malicious Code protection infrastructure is updated to address the new risk, must be in accordance with Virus/Malicious Code Contingency Plan.

A process to ensure that Virus/Malicious Code detection infrastructure remains active and is not disabled at any potential entry point shall be implemented.

Associated Procedures

The IT Department should install Virus/Malicious Code protection software (e.g. Anti-Virus Software) on all PC's, servers, electronic mail servers, Internet gateways etc. Prior to moving these to production the IT Department should ensure the anti-virus signatures and engine versions are updated with the latest vendor patches.

Once updated, a full system scan and clean should be run prior to handing the PC to users and a daily update schedule should be configured and real-time scan should be running all the time. Then the IT Department should brief users receiving the PC as an owner on how to maintain the anti-virus in case asked to and should remind users of the safe use policies as applicable.

The IT Department should ensure that the Virus/Malicious Code detection infrastructure is updated daily or as soon as the latest product and Virus signature updates are released.

Additionally, the IT Department should regularly collect information from qualified sources such as subscribing to reliable mailing lists and/or checking vendor web sites giving information about new.

Virus/Malicious Code

The IT Department should develop a Virus/Malicious Code Contingency Plan that guides users on how to update their anti-virus agents if the main anti-virus local server is not accessible for any reason.

User Responsibilities

Users must be prohibited from changing the configuration of, removing, de-activating or otherwise tampering with any Virus/Malicious Code prevention/detection software that has been installed on systems used by them.

It is the responsibility of users to ensure that all anti-virus updates made available to them are immediately implemented on the workstations, desktops, and laptops and other equipment as directed by the IT Department.

Associated Procedures

The IT Department should restrict users privileges from changing the configuration of, removing, de-activating or otherwise tampering with any Virus/Malicious Code prevention/detection software that has been installed on systems used by them.

In case where the main anti-virus local server is not accessible, the IT Department should ensure that anti-Virus updates are made through the internet. The IT Department should then check if users have installed those anti-Virus updates within the specified timeframe. If users are not aware of how to install such anti-virus updates, the IT Department should help the users in installing them. Although server-based anti-virus solutions collect all anti-virus detection and cleaning incidents centrally, users should report all incidences of Virus/Malicious Code (detected by the installed Virus/Malicious Code protection software) immediately to IT Department to enable timely remediation.

Additionally, users should ensure that media exchanged with other departments and organizations are checked for Virus/Malicious Code.

Detection of Virus/Malicious Code on LCB Finance's Information Systems

All possible and practicable measures shall be taken to detect Virus/Malicious Code on LCB Finance's information systems infrastructure. These measures would include but are not limited to the following:

- Implementation of memory resident components of Virus/Malicious Code detection software in PC's, servers, laptop computers and other appropriate components of LCB Finance's information systems infrastructure.
- The steps/decisions to be taken in the event of the entry of a Virus/Malicious Code into LCB Finance's information systems infrastructure, shall be in accordance with the Virus/Malicious Code Contingency Plan.
- A process to ensure that Virus/Malicious Code detection software remains active and is not disabled on any component of LCB Finance's information systems infrastructure shall be implemented.
- Virus/Malicious Code protection software scans shall be performed on all PC's, servers, laptop computers and other components of LCB Finance's information systems architecture at periodic intervals to detect potential Virus/Malicious Code.

Associated Procedures

The IT Department should implement a Virus/Malicious Code Contingency Plan to overcome any incident of a Virus/Malicious Code infecting LCB Finance's information processing facilities.

The Virus/Malicious Code Contingency Plan should contain procedures to:

- Inspect the extent of information processing facilities infected
- Disconnect infected machines from the network
- Immediate external isolated back up of data of the infected facilities to check for infection and not to spread the Virus/Malicious Code into the uninfected back up facilities
- Removal of the Virus/Malicious Code
- Disinfecting the facilities and their separate back up
- Updating Virus/Malicious Code detection system
- Resuming operation on the facilities

Additionally, the IT Department should ensure that the users have not changed the Virus/Malicious Code protection software configuration and should ensure that the anti-virus agent is running all the time on the user PC by pulling the agent status every 5 minutes. If the agent is detected unreachable while the PC is reachable that means the agent is not functioning and accordingly the anti-virus server should block all network access to that PC until the agent is running again.

For non LCB Finance owned PCs requiring access to LCB Finance network, the LCB Finance department hosting the third party should contact the IT Department to ensure that their PCs are scanned and cleaned from any virus/malicious code prior to allowing any network access. The IT Department should perform weekly scans to detect potential.

Removal of Virus/Malicious Code from LCB Finance's Information Systems

All Virus/Malicious Code identified in files downloaded from the internet or email systems or introduced via floppy disks or CD-ROMs or through any other media or interconnection/networking facility shall be removed.

Associated Procedures

Where Virus/Malicious Code is identified/detected:

The IT Department should immediately isolate the infected system from the network infrastructure and handle it in accordance with the Virus/Malicious Code Contingency Plan. Accordingly, the IT

Department should remove the Virus/Malicious Code using appropriate software if the anti - virus agent installed could not remove it.

At the same time, the IT Department should conduct a comprehensive Virus/Malicious Code scans of all components of the Information Systems Infrastructure to detect any further cases of infection. The comprehensive scanning should be configured to scan all compressed files and system libraries to the maximum levels supported by the anti- virus product.

Also, the IT Department should investigate the path used by the Virus/Malicious Code to enter the network and appropriate prevention measures should be implemented to prevent recurrence. Anti-virus products offer detailed logging that the IT should configure to capture the maximum level of detail and should configure the purging intervals only annually or never as needed. These Logs should be backed up and should be available for any investigation requirements in case of virus/malicious code attack incidents.

Operations - Malware protection on servers & end user device

An enterprise level virus guard is installed on all servers, desktops, laptops etc. and license is renewed annually. It is centrally managed and it is up-to-date anti-spam and anti-malware protection.

Before performing a version upgrade of a virus guard, it is tested on a staging environment. Finally,it is deployed for servers and end point user devices. The Virus guard version upgrade is centrally managed and manual deployment will be done if there is any network issue.

All the hired or leased PCs is equipped with AV software before handing over to the users. End user device connected to the AV software through the Network Agent. IT department monitor the anti-virus status of all servers and end user device daily basis. Issues are rectified through and if it is difficult, it will be resolved through local machine.

In AV software, separate groups are created under manage device for applying difference protection policies.Protection policies are defined according to the user privilege. Virus definition update is centrally managed, and it is deployed through AV software to the servers and end point user device. Once update is released, it will push the update to end point user. Miss task is enabling for virus definition update.Online update is enabling when users are not connected with network.

Scheduled full scan is enables for full scan on Friday 12.30 PM and miss task is enable for it.

Quick scan is enabled for external storage devices and it will be run automatically. Finally, we can see the report of scan task. On demand scan is activated for all user PCs and servers therefore user will be able to do custom scan.

User is not allowed to stop virus scan task and exit or disabling virus guard is not allowed as these functioned are password protected.

Type of reports

- Anti virus database usage
- Error reports
- Lab software version report
- License usage report

- Most infected computer usage
- Network attack report
- Protection coverage reports
- Protection status report
- Report on application registry
- Users of infected computers report
- Viruses report

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy

External References

- ISO / IEC 27001-(1/2)
- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department.

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or Director Finance , depending on the criticality. The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

8. MOBILE DEVICE MANAGEMENT

PURPOSE

This document develops to assist the LCB Finance by providing a document of minimum standards, procedures and restrictions for end users who have legitimate business requirements to use of Mobile devices within the entity. This procedure must be used as guidelines to comply with applicable policies in order to ensure integrity, confidentiality and availability of the Mobile devices and related services.

INTRODUCTION

The Entity will identify that data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to the entity public image. According to acceptable user policy, entity will not allow and limited to, all devices and devices accompanying media in entity network resource that fit the following device classifications:

- Laptop/notebook
- Tablet computers such as iPads
- Mobile/cellular phones
- Smartphones
- PDAs
- Any mobile device capable of storing District data and connecting to an unmanaged network.

But entity will allow and not limited to, store to use the business email facility on their devices by using their mobile networks for doing so.

SCOPE

This SOP includes guidelines applies to all the mobile devices and related services which are used in the LCB Finance technology resources. It is the responsibility of each system User to follow the standard. This Policy covers all mobile devise and services operated by the entity and/or contracted with a third party by LCB Finance.

All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her system administrator, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy.

OBJECTIVES

- Implement process to identify the users who access entity email service and the users who willingly to use mentioned services.

DEFINITIONS

Mobile device management (MDM) is a type of process used by an IT department to monitor, manage and secure employees' mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems being used in the organization.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Executive - IT

SPECIFIC PROCEDURE

Create signed agreements with MCT users

The MCT user should be entered into a written agreement for every type of MCT use, whether the employee teleworks regularly or not. The parameters of this agreement should include certain key elements. Most importantly, the agreement should be signed and dated by the Head of IT. The Head of IT should keep copies of all MCT agreements on file.

MCT agreements should be revisited by the Head of IT and the MCT user and re-signed on a periodic basis, preferably at least once a year.

Base denials on business reasons

MCT requests may be denied and MCT agreements may be terminated. MCT is not an employee right, even if the employee is considered "eligible" by LCB Finance standards and/or the individual agency standards. Denial and termination decisions must be based on business needs or performance, not personal reasons.

Associated Procedure

LCB Finance IT should;

- Maintain a MCT device inventory, update immediately when a change occurs.
- Thoroughly review all MCT agreements to ensure they are in compliance with Information Security Policies and Procedures.
- Ensure MCT users receive information systems security training.
- Work with employees to ensure that they fully understand the MCT usage and have the technical expertise to adhere to LCB Finance security requirements.
- Invest in technology and equipment that can lead to successful implementation and secure operation of MCT.
- Enforce personal privacy requirements for records.

MCT usage and users security responsibilities

A formal process is required to be developed and established to safeguard and prevent leakage of information through mobile devices such as Mobile phones, Laptops and Tablet PCs. It shall include, but not be limited to the following,

- If the mobile device contains confidential information, access must be protected via the user authentication (e.g., user ID and password) and inactive session timeout controls.
- Mobile devices are easy to spot and are prime targets for theft. It shall be the employee's responsibility to ensure every effort is taken to protect LCB Finance mobile devices, whether in the office or when travelling.
- If a mobile device is stolen, the proper local police officials need to be notified.

- A copy of the police report should be obtained, and provided to the LCB Finance IT.
- Employees are required to have management approval to connect any mobile device (other than company owned computers) to the LCB Finance network. Only devices certified by LCB Finance may be used on supported desktops.
- Any use of public and/or private wireless networks, when accessed with a LCB Finance device, shall be in accordance with local laws.
- No LCB Finance equipment shall be connected to non-LCB Finance networks without appropriate security controls such as personal firewalls and anti-virus software.
- Participation in LCB Finance information systems security training.
- Complying with LCB Finance Information Security Policies and Procedures and with any additional requirements mentioned in the MCT agreement.

Password protection

Power-on password protection is the first step toward securing data on mobile devices. MCT devices should be enabled with password protection according to LCB Finance's password policy. Without providing correct inputs for user name and password, the device should not allow to the user to log in.

The MCT device should be configured in such a way that it locks after a predefined number of failed password entry attempts. Complete device disablement should be enforced after the failed password entry attempts. Quality password use should be configured for MCT devices. Further, frequency of password change requirements needs to be enforced on MCT devices.

Device data encryption

Technical solutions should be implemented on MCT devices to encrypt data that resides on devices. In the case of a lost or stolen device, data is protected through strong encryption, rendering the device unusable. Removable storage media, such as compact disks, USB drives, should also be encrypted.

The following should be considered for encryption,

- Full disk encryption for Win32
- Full 128 bit encryption for both device and over-the-air transmission (e.g., WPA-2)
- The option to encrypt personal data, company specific data or data stored on external media

Data fading

To eliminate manual IT intervention for lost or stolen devices, automatically rendering a device unusable should be promoted. Software with the capability of locking, wiping or resetting a device that has not communicated with the corporate network after a predetermined number of days should be implemented.

Antivirus, personal firewall and patch management

Antivirus definitions should be updated and the system should be scanned on a regular basis. Personal firewall should be installed on MCT devices, which should be configured in such a way that it minimises internal and external attacks, protects data privacy and eliminates unwanted sources of network traffic.

Personal firewall installed on MCT devices should provide features such as state-full inspection and protocol filtering and should provide several levels of control over the kinds of information that users, web browsers, instant messenger programs and email clients can send over the internet.

Patch updating should be configured in such a way that the patches are being updated on MCT devices only from corporate the LAN. No MCT device should be configured for automatic patch updating. This ensures only tested patches are being installed on MCT devices.

Protect lost or stolen devices

The small size and portability of mobile devices, and their removable memory sources make them more vulnerable to loss or theft. When this happen, it is critical that strong access controls and data protection measures are already in place on the device to protect against unauthorized data and network access. Software ensuring the security of mobile data should be deployed for protection of mobile devices. At a minimum, this software should have the following capabilities;

- Power-on password protection
- Data encryption both locally on the MCT device, and on removable media
- Access logging and auditing
- Over-the-air data wiping
- Data backup and restore (for data recovery in the event of loss)

General Procedure – Email Facility for Mobile Devices

Identify users who used email facility on their mobile devices - The IT department will maintain the deployment register for future reference and assist.

Assist the user who willing to store email facility on their mobile devices - IT department in coordination with the users, based on the aspects mentioned above and do the deployment process of applying application and update the email deployment register accordingly.

FORMS/TEMPLATES TO BE USED/REFERED

Email deployment List for mobile devices

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Acceptable user policy

External References

- ISO / IEC 27001-(1/2)
- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets

- Termination of Employment
- Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

This policy is intended to address Operating Systems Security requirements. Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or Director Finance, depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months). At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

The waiver shall be monitored to ensure its concurrence with the specified period for any exceptions.

All exceptions to this policy must be communicated through the Policy Waiver Request Form.

9. NETWORK & FIREWALL MANAGEMENT

PURPOSE

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the internal and external networks are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards. Furthermore, LCB Finance operates perimeter firewall between the Internet and its private internal network in order to create a secure operating environment for LCB Finance's computer and network resources. A firewall is just one element of a layered approach to network security.

INTRODUCTION

This document provides LCB Finance with Consistent standards for network access and authentication. Any user accessing the LCB Finance's corporate network has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network. Apart from that LCB Finance's firewall perform a huge role to secure LCB Finance's information and other business critical systems form any malicious attacks.

SCOPE

This SOP includes guidelines that must want to follow all users who have access to LCB Finance-owned or LCB Finance-provided computers or require access to the corporate network and/or systems. Further this policy defines the essential rules regarding the management, maintenance and operation of network firewalls at LCB Finance and applies to all network of LCB Finance.

This policy applies not only to employees, but also to guests, contractors, and functional units in LCB Finance regardless of the geographic location that requiring access to the corporate network. Public access to the LCB Finance's externally-reachable systems, such as LCB Finance's corporate website or public web applications, are specifically excluded from this policy.

OBJECTIVES

- Ensure the protection of the network from unauthorized access and protect information from unauthorized disclosure and accidental modification.
- Ensure the accuracy and completeness of the LCB Finance's network assets.
- Implementation of network documentations within the LCB Finance, the network documents should include:
  - Network Diagrams
  - System Configuration
  - Firewall Rule set
  - IP Addresses
  - Access Controls List
- Network segmentation is implemented to ensure trusted and untrusted networks are separated.
- Ensure firewall maintenance (including applying updates and updating of rules) is performed by operational procedures and controlled by Change management process.
- To ensure firewall event logs are reviewed periodically and deviations are treated as a security incident.
- To ensure user activity and system events on business critical systems and -processes are logged and monitored.

- To evaluate effectiveness of each control, protecting the Confidentiality, Integrity and Availability is tested annually.
- To ensure Vulnerability management policies and procedures are in place.
- To evaluate Vulnerability scans are ran across servers at least annually.
- To ensure a risk classification matrix is used to discover and classify vulnerabilities on servers, network and firewall.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Assistant Manager – IT IT Executive

SPECIFIC PROCEDURE

Network Security Management

9.1.1.1. Network Controls

- LCB Finance shall implement appropriate security measures and features, to protect the network and system infrastructure.
- Controls shall be implemented to protect connected systems, and to safeguard the confidentiality and integrity of critical business information assets that pass over public networks.

Associated Procedures

The Head of IT should establish appropriate controls to protect the network and system infrastructure. Defined controls should enable reporting status of all network components and devices. Also, network management tools that provide protocol anomalies, traffic analysis, hardware malfunction signals, etc should be used to monitor and maintain the network as and when required.

9.1.1.2. Security of Network Services

Network services agreement shall be defined for network services provided in-house or through third parties and shall include security features, management requirements and service levels.

Associated Procedures

The IT Department should regularly monitor the ability of network service providers to provide and manage agreed services in a secure way and in accordance with service level agreements Also, the IT Department may conduct penetration testing for the network service provided in coordination with the provider and should obtain a formal consent on the penetration activity or incorporate such authority. Once the test is concluded, test results should be documented and officially communicated with the service provider to remedy any security issues in violation of agreed A security arrangements grace period according to the A should be given to the vendor to recover and correct any security issues.

Then, the IT Department may conduct another penetration test (if required by another party) to verify that communicated security issues were addressed and corrected by the service provider.

Network Access Control

9.1.1.3. Policy on Use of Network services

- Access to networks and network services shall be specifically authorized in accordance with LCB Finance's Logical Access Security and IT Asset Management policies and associated procedures.
- Access to networks and network services shall be controlled on the basis of business and security requirements, and access control rules defined for each network.

Explanation

These rules shall take into account the following:

- Security requirements of the network or network service(s)
- An identified business requirement for the user to have access to the network or network service ('need-to-have' principle)
- The user's security classification and the security classification of the network/network service (IT Asset Management Policy)
- Legal and/or contractual obligation to restrict or protect access to assets
- Definition of user access profiles and management of user access rights throughout the network of LCB Finance.
- Logical access to networking hardware and software shall be limited to properly authorized personnel.
- Access to programmable network devices (e.g., routers, switches and firewalls) must be restricted to authorized IT employees.
- The use of network diagnostic and security tools must be limited to specifically designated staff, and in accordance with their job responsibilities.
- Access to all network configuration and security-related data (e.g. dial-up numbers, IP addresses) must be limited to authorized users.

Associated Procedures

Head of IT with support of his staff should configure routers and switches to prevent the disclosure of the configuration of the internal network to external and unauthorized entities. Head of IT should enable unattended network connection ports (i.e., conference rooms, empty offices, etc.) only when needed. Network assigned addresses should be controlled and segmented into category ranges (i.e. server farm address range, network printer range, desktop range, laptop range, etc.) Addresses should be reserved to corresponding devices MAC addresses using the network switch port configuration utilities and the server based DHCP.

Proper labelling of all network components and devices should be done systematically and is key to easy and effective network troubleshooting. Once configuration plan is decided and labelling of all network attached devices and components are concluded, listing of each device, and component cross-referenced with assigned user, network address etc. should be developed and maintained as changes take place; the list should be treated confidentially. In addition, Unattended network nodes should be physically disconnected from the network cabling cabinet patch panel and should be connected only upon authorized requests or upon assigning to new device. The IT Department should ensure that access to network devices, tools and services is authorized and in accordance with LCB Finance's information security policies

9.1.1.4. User Authentication for External Connections

- Remote user access to LCB Finance's networks shall be subject to appropriate user authentication methods
- Dial-Up access to LCB Finance's resources shall be in accordance with LCB Finance's Access Control Policy and IT Asset Management Policy and associated procedures.

Associated Procedures

The user authentication method used will depend on the user's security classification and the security classification of the network and the network service to be accessed. As such, information asset owners should authorize dial-up access to LCB Finance's resources and Head of IT should approve such access.

The Head of IT should also authorize attachment of analog data lines to computers on LCB Finance's information network upon receiving the Head of Department approval. The Head of IT should implement appropriate authentication and cryptographic controls for remote access to internal network.

9.1.1.5. Equipment Identification in Networks

Authentication shall be at the application or network level

Associated Procedures

Head of IT should ensure that the equipment authentication is performed at the application layer or the network layer of the OSI model Simple Network Management Protocol and other network management protocols/tools should be used for network equipment identification and monitoring.

Accordingly, network administrators should configure the SNMP domain or segment according to the required segmentation of network equipment grouping for ease of management and monitoring and also for protection from default protocol domains exposures.

9.1.1.6. Remote Diagnostic and Configuration Port Protection

- All remote diagnostic connection for maintenance, support and special services (like administration) must be secured and controlled.
- Only the authorized maintenance and support personnel shall be authorized to access the diagnostic and configuration ports. This connectivity shall be provided only as and when required. After usage, it shall be disabled.

Associated Procedures

Network Administrators should obtain authorization in accordance with change management procedures before accessing remote diagnostic and configuration ports (refer to the Change Management Policy) Accordingly, the Head of IT should authorize any remote management tools and in what context they should be used

9.1.1.7. Segregation in Networks

- LCB Finance's information systems network must be divided into logical segments based on the access requirements. The criteria for division of networks shall also consider the relative cost and performance impact of incorporating suitable technology.
- Internal network shall be segregated from the external network with different perimeter security controls on each of the networks.
- The connectivity between internal and external networks shall be controlled.

Associated Procedures

The IT Department in coordination with the information asset owners should ensure that appropriate controls are in place to segregate and control connectivity between internal and external networks Accordingly, the Head of IT, based on business requirements should propose a comprehensive perimeter protection security plan that should be reviewed and authorized by the IT Steering Committee Once authorized, the IT Department should carry out the implementation either internally or via the assistance of third parties

9.1.1.8. Network Connection control

- A Service Policy Table shall be formulated for each service that is allowed through each firewall
- Users shall only be provided with the direct access to the services that they have been specifically authorized to use.
- Users shall not use dial-up modems for external connectivity, while they are connected to LCB Finance's internal network.

Associated Procedures

Assistant Manager IT should develop Network Service Policy Table and configure firewalls based on that table.

Once that table is completed it should be sent to the Head of IT and information asset owners Upon receiving the table, information asset owners and the Head of IT should approve Network Service Policy Table Accordingly, Assistant Manager IT should block any services that are not required, preferably at the firewall, but at least at the end system or server. Additionally, Assistant Manager IT should document and obtain authorization from the Head of IT for all external connections by business partners and customers in accordance with the defined procedures.

The IT Department should obtain detailed descriptions of the security attributes of all external value added services used (if any) from external Network services providers. This description should establish the confidentiality, integrity, and availability of business applications and the level of controls (if any) required to be applied by LCB Finance In addition, the IT Department should ensure that the description of the security controls is included in the agreement of the service with Network services providers

9.1.1.9. Network Routing Control

- Appropriate routing control mechanisms shall be deployed to restrict information flows to designated network paths within the control of LCB Finance.
- Network routing controls as a minimum shall be based on positive source and destination address checking mechanisms.

Associated Procedures

Network Administrators should implement controls to ensure that flow of data and information is restricted and controlled by properly configuring routing tables and gateways Additionally, routing traffic should be authorized by the Head of IT based on business communications needs and in coordination with business process owners whom should inform the IT Department of any connectivity requirement with ample time to plan, procure and deploy the connectivity and configure related routing settings.

Firewall Configurations Management

9.1.1.10. Baseline security set

- The firewall should not have any additional services running that can be accessed remotely. Any additional service such as SMTP and DNS running on the firewall machine would present the attackers with an opportunity to compromise the firewall by exploiting vulnerabilities associated with the service.
- All default vendor supplied user accounts should be disabled after setting their password to a complex value.

9.1.1.11. Firewall interfaces

- The firewall should segment the network based on the risk levels. Systems with similar risk levels should be put into one segment. For example, if the firewall is segregating the internal network from the internet there should be a minimum of three segments-one for internet, one for internal network and one for machines that are accessed from both the internal network and the internet.
- The Head of IT will be responsible for determining the number of segments and the servers that will be located in each segment. Approval should be obtained from the Head of IT before adding or removing servers/applications to/from a firewall segment.
- Listed below are guidelines to adhere while determining the number of firewall segments and servers/applications to be hosted within that segment;
- Sensitive and critical applications/servers that are accessed only internally should be hosted on the most protected segment of the firewall.
- Systems accessed internally as well as by external sources should be hosted on a separate segment of the firewall, preferably the De-militarized Zone (DMZ). Additionally, for better manageability, these systems can further be classified into business application and infrastructure support applications (e.g., DNS, Web mail, Proxy), with each category hosted in a separate DMZ.
- Connection links from third parties, etc., should terminate on a separate interface of the firewall.
- Wide Area Network (WAN) links connecting to the data center should terminate on a separate interface of the firewall.
- Administrators normally require unrestricted access to systems and networks they manage. In case these administrators have their machines configured as part of the user LAN, there is the strong possibility that a malicious user may sniff the administrative communication and thereby gain unauthorized administrative access. To avoid this, it is necessary to group all administration terminals on to a separate interface of the firewall with access restricted only to administrators. Additional security measures such as dual factor authentication should be considered for protecting these terminals.

9.1.1.12. Rule base creation

The Head of IT is responsible for designing and testing the firewall rule base before deployment in production. The Assistant Manager–IT should obtain the required inputs from the respective application

owners for designing of the rule base. The following guidelines should be adhered to while adding or modifying the rule base,

- By default, the firewall MUST have a DENY ALL policy, with access granted on a need to do basis. The firewall should have a rule to deny all access that is not explicitly allowed.
- Only required services/ports must be opened between specific source and destination IP addresses/subnets. Use of the "ANY" literal either in the source, destination or service/ports must be strictly avoided.
- The firewall rule base should restrict access to required ports on the target machine. The source field in the rule base should be restricted to specific IP addresses/subnet addresses wherever feasible. In the case of applications where the number of individual IP addresses/subnets is very large the source address can be made generic to make the rule base more manageable.
- Application/servers which are directly accessed from a public network such as the internet should be moved to a separate segment (Demilitarized Zone) of the firewall. The IP address of the server should be NATed with a public IP address.
- For connections with third parties, NATing should be performed using any available private/public address slot.
- Access to administrative ports including SSH and Microsoft Windows Terminal services on protected servers should have user ID based authentication at the firewall in addition to the source IP address. User authentication provides additional security and also provides the facility for authenticating roaming users.
- The firewall user-database, needed for rules that are configured for user authentication, can be stored either locally on the firewall or in an external directory server. Password policies for these user accounts including password expiry, password history, and password complexity should be enforced. Account lockout should be configured to prevent password cracking attempts. It should be ensured that these user credentials are transmitted in encrypted format from the user PC to the firewall.
- The rule base should be approved by application owner and should come through CR form (Change Request) prior to deployment. The Head of IT should give a copy of the tested rule base pertaining to the application to the respective application owners. This will ensure that application owners are aware of the services that will be allowed through the firewall prior to deployment. This will also help in reducing troubleshooting efforts when the firewall goes into production.
- For certain applications such as MySQL, Active FTP uses random ports for data transfer between the client and server, after the initial handshake has taken place over a standard port. Using such applications demands opening all ports between the client and server for successful communication. For such access requirements, the following steps should be followed to avoid exposing all standard TCP/UDP ports,
- Create a service group for the application consisting of the standard port for initial communication and all higher end TCP/UDP ports (1024 and above)
- Service = Standard port + (1024 – 65536)
- Open access for the service group between the desired client and server
- As enabling logging will generate voluminous data, enable logging on the individual rules judiciously.
- The comments column for each rule MUST have the following information duly entered,
- Purpose of the rule
- Expiry date, for temporary rules
- The LAST rule for each segment MUST be a "DENY ALL" rule denying all traffic not explicitly allowed. Logging should be enabled on this rule.

9.1.1.13. Rule base change

- After the firewall goes into production, all changes to the rule base should be done after proper authorization, to ensure that the security level is maintained at all times. Users should contact the application owner for any access requirement. Application owners should validate the request, translate the user request to specific IP address and port numbers and pass it to the Head of IT.
- A backup/recovery strategy should be in place to ensure that an implementation failure does not adversely impact availability of other systems and firewalls, in general.
- In situation where the exact access requirements are not known (e.g., exact ports to open between source and destination IPs), changes can be implemented by initially enabling more access and enabling logging. The logs should then be used to verify the exact port requirements. The activity of fine tuning the ports based on firewall logs should be completed within six hours of enabling, as there is risk of unauthorized access during this time.

9.1.1.14. Administrative access

- Administrative access to firewalls is required for activities including rule base modification, firewall-user account management, firewall-administrator account management and log monitoring. Super-user privileges should be provided to members of the IT security team on a need to have and need to do basis.
- Default passwords for all vendor-supplied user accounts should be changed to complex combinations. Logical access to the firewall should be limited to the Assistant Manager – IT and/or to a person appointed by the Head of IT. Each Systems Administrator should have separate account within, for management. Local system administrators should not have access to firewall applications. Administrator accounts on the firewall should have the password policy and account lockout configured.
- Access to firewall administration programs should be through encrypted channels. If the firewall software itself does not provide this facility, then additional mechanisms such as IPSEC should be used for this purpose.

9.1.1.15. Audit Logging

- Logging needs to be enabled to ensure that all critical access is tracked. Logging should be enabled for rules enabling administrative access (e.g., SSH access to web server). Logging should not be enabled for normal user access (e.g., HTTP access to web server).
- Logging should be enabled for the last rule that blocks all access that is not explicitly allowed by the other rules.
- Logging should be enabled to track any changes done to firewall configurations including changes to the rule base. This will ensure that all changes can be tracked for trouble shooting as well as for audit purposes.
- The Head of IT should monitor the logs periodically (at least once in three months) for the following activities,
- Port scans
- Authentication failures
- Denial of service attempts
- Failed connections

9.1.1.16. Performance monitoring

- Resource utilization should be tracked to ensure that the firewall is performing at the optimum level. The Assistant Manager – IT and/or a person appointed by Head of IT should monitor the critical system parameters on a continuous basis. Any surge in utilization of any of these parameters might be an indication of a system under attack. The IT Security team should determine threshold levels for peak and average usage for the following parameters,
- CPU utilization

- Memory utilization
- Hard disk free space
- Concurrent connections

9.1.1.17. Change control

- Changes to the following should adhere to the change management process
- OS Upgrade/installing a new patch on the firewall
- Firewall Application upgrade
- Installation or removal of additional component
- Integration of Firewall with third party components
- Adding a new segment or modifying existing segment
- Adding a new Firewall Rule
- All the Firewall changes should be approved by the Head of IT prior to the implementation and The Assistant Manager – IT and/or a person appointed by Head of IT should be responsible for implementing the changes on the firewall.

9.1.1.18. Backup and recovery

The Executive – IT and/or a person appointed by Head of IT will be responsible for backup and recovery of the firewall. The following should be backed up soon after installation and successful testing of the firewall, and securely stored,

- Firewall OS files
- Firewall application files
- Configuration files
- Firewall rule base
- Routing table
- Firewall logs

A full backup of firewall application/operating system files should be taken before any major changes to the firewall, including;

- Upgrade of firewall OS/application
- Installation of any additional component on the firewall (e.g., VPN, Hard disk drive)
- Integration of the firewall with third party components (e.g., integration of firewall with RSA for authentication) ▫ Adding a new firewall interface
- Backup of firewall logs and audit trails should be taken on a daily basis and archived for a period of **at least six months** to meet statutory requirements and for forensic analysis.
- Backup of the firewall policy/rule base should be taken before and after addition of new rules or modification to any existing rule.
- By default, a backup of the firewall configuration and policies should be taken on a monthly basis, irrespective of whether changes are made to the firewall or not.

9.1.1.19. High availability

Firewall redundancy should be configured based on the criticality of the applications and network segments/zones being protected. For critical applications/zones, firewalls should be configured in high availability mode to ensure minimum downtime for the respective applications.

All communication between the primary and secondary firewall appliance should be secure using supported encryption technologies and dedicated communication channels such as cross-over cables.

9.1.1.20. Documentation

The IT team should maintain detailed documentation of the firewall architecture and administration tasks.
Firewall architecture documentation should include the following,

- Network diagram with firewall segments/interfaces
- IP addresses of firewall interface and network devices connected to the firewall
- Routing table of firewall and connected devices
- Documentation on firewall administration tasks should include the following,
- Installation and configuration of the firewall
- Adding/deleting/modifying the firewall rule base
- Adding/deleting/modifying the firewall routing table
- Adding/deleting/modifying the firewall users
- Adding/deleting/modifying the firewall administrators
- Backup/recovery of the firewall OS/application files
- Backup/recovery of the firewall rule base
- Backup/recovery of log files
- Backup/recovery of user databases

Audit Policy for Network & Firewall Management

Auditing is very important to understand the operational and Security issues. Hence proper configuration is mandatory to get the exact information required.

Audits should be conducted to:

- Ensure integrity, confidentiality and availability of information and resources.
- Investigating possible security incidents to ensure conformance to LCB Finance's
- Information security policies.
- Monitor user or system activity where appropriate

9.1.1.21. Audit Policy Recommendations

Audit Policy	Domain Controllers	Member servers	Workstations
Audit account logon events	Success, Failure	Success, Failure	Success, Failure
Audit account management	Success, Failure	Success, Failure	Success, Failure
Audit directory service access	Success, Failure	N/A	N/A
Audit logon events	Success, Failure	Success, Failure	Success, Failure
Audit object access	Success, Failure	Success, Failure	Success, Failure
Audit policy change	Success, Failure	Success, Failure	Success, Failure
Audit privilege use	Not configured	Not configured	Not configured
Audit process tracking	Not configured	Not configured	Not configured

Audit system events	Success, Failure	Success, Failure	Success, Failure

These events are logged in the event viewer.

The event logs should be checked weekly on domain controller to see if any violation has been made and necessary actions taken. The domain controllers should be audited to check for accounts having domain admin rights, Global membership and verified whether they are approved accounts by the Head of IT. The Domain account policy should be audited weekly and recorded in a register. If any change is recommended, it has to be approved by the Head of IT and the Assistant Manager – IT. Any Dormant/Inactive/Generic accounts should be checked on the domain controller once in a month. If such accounts are found that are not approved should be removed immediately. Event logs should not be deleted. They should be kept for a minimum of 90 days.

9.1.1.22. Auditing Software

LCB Finance's network should be scanned weekly using standard software provided by Microsoft called Microsoft Baseline Security Analyzer (MBSA) or any auditing tool as recommended by Security.

9.1.1.23. Auditing Result

The Auditing result should show information on

- **Local administrator Accounts in all systems**
  These details should be recorded in a register and if exceptions found should be logged. All exceptions should be approved by Head of IT.
- **Password expiration of all accounts residing on systems**
  Non-expiry passwords if found and marked as exception should be approved by Head of IT, otherwise they should be configured to comply with password policy.
- **File System information**
  All File systems should be NTFS and any issues should be logged and fixed.
- **Restrict Anonymous**
  This if found enabled should be disabled.
- **DCOM Vulnerability**
  This vulnerability if found should be recorded and fixed immediately.

9.1.1.24. Additional System Information

- **Unnecessary Services**
  Auditing checks if some potentially unnecessary services are running. Such services if found should be disabled.
- **Shares**
  It checks if any shares are created by users on their PCs. They should be removed if found.
- **Macro Security**
  It checks for any macro security vulnerability. Appropriate office update patches should be installed to rectify it.
- **IE Zones**
  It checks if the systems are configured in a secure IE zone. If found to be different it should be reset to medium.
- **Member Servers/ PCs**
  To capture events on Member Servers/PCs, audit policy should be configured with a GPO linked to the container within which these computer accounts reside. All the Event logs should be recorded

on the local PCs and member servers for operational and security issues for minimum of 90 days AS configured.

- **Random System Audit – Every Month**
  At least two PCs should be chosen at random and audited for the following. The audit report should be sent to LCB Finance management and the Head of Department of the member to whom the PC is allocated.
- **Unauthorized Software**
  The software's installed on the system should be checked to see that they are licensed and not unauthorized. If any unauthorized software is found it should be removed and the user should be advised not to install any freeware and sharewares. Software's installed on PCs for evaluation and testing purpose should be authorized by the Head of IT. All such requests for installation should mention clearly the business reason and number of days it will be used after which the IT support team should uninstall it.
- **Access to Unauthorized Websites**
  Sites browsed by users should be checked, to see that inappropriate sites like astalavista.com, rediff.com and personal mail accounts like Yahoo mail, hotmail, rediff mail etc. should not be visited. Users should be advised not to browse sites that are not related to business needs.
- **Data Not Related to Business**
  Presence of MP3, JPEG, and AVI files etc. on the system should be checked. If found, they should be deleted and users advised not to keep any files not relating to LCB Finance business on their PCs.
- **Mails**
  Sent Items in User mailboxes should be checked to ensure that no LCB Finance's confidential data is sent outside the domain. All incoming and outgoing mails should be logged at the server level to ensure confidentiality and integrity
- **Groups**
  Groups and User IDs on the local machine should be checked to make sure that no unauthorized User ID is present in the Local admin and Power User group
- **Vulnerability Review**
  The main deliverable of the Audit should be a detailed report, which the IT Team would use to address key noted weaknesses of the operations. The weaknesses noted may become audit issues with the appropriate follow-up as necessary.
- **Penetration Test**
  Penetration testing should be done to actively assess information security measures. The results of the assessment should be documented and corrective strategies should be derived.

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Change Management Procedures
- Passwords & Lockout Procedures
- IT Asset Management Procedures

External References

- ISO / IEC 27001-(1/2)

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT and/or CEO, depending on the criticality. The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

10. OPERATING SYSTEM MANAGEMENT

PURPOSE

This document develops to assist the LCB Finance by providing a document of minimum standards regarding the use of OS's including Client's OS, Server OS's and Server OS's within the entity. This procedure must be used as guidelines to comply with applicable policies in order to ensure integrity, confidentiality and availability of the Operating Systems.

INTRODUCTION

OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS guarantees must follow the specified the steps which used to protect the OS and preventive control techniques. This document will provide the entity, standards and procedures for the safeguarding OS security in order to perform required tasks and stop unauthorized interference. The below mentioned processes will be carried out ~~carry~~ in terms of Operating Systemsecurity.

- OS installation: initial setup and patching
- Remove unnecessary services, application, and protocols
- Configure users, groups and authentication
- Install additional security controls
- Test the system security

SCOPE

This SOP includes guidelines applies to all the OS's and the Applications which are used in the LCB Finance technology resources. It is the responsibility of IT Department to follow the standard. This Policy covers all Operating Systems (OS) environments operated by the entity and/or contracted with a third party by LCB Finance.

All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her system administrator, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy.

OBJECTIVES

- Implement procedures to periodically assess the current level of install OS and perform regular OS patch updates.
- Implement procedures to periodically assess the current level of install Network OS and perform regular OS patch updates.
- To access all installed application software, services and protocols.
- To access the update procedure of application software and validation including antivirus guard.
- To access the granted account privileges including configure users, groups and authentication
- Scrutinizing all incoming and outgoing network traffic through a firewall
- Test the security of the basic operating system to ensure that the steps taken adequately address its security needs

DEFINITIONS

Operating System

An operating system (OS), is system software that allows a user to run other applications on a computing device. While it is possible for a software application to interface directly with hardware.

The OS manages a computer's hardware resources, including:

- Input devices such as a keyboard and mouse
- Output devices such as display monitors, printers and scanners
- Network devices such as modems, routers and network connections
- Storage devices such as internal and external drives

The OS also provides services to facilitate the efficient execution and management of, and memory allocations for, any additional installed software application programs.

Server Operating System

A server operating system, is an operating system specifically designed to run on servers, which are specialized computers that operate within a client/server architecture to serve the requests of client computers on the network.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Assistant Manager IT, IT Executive

SPECIFIC PROCEDURE

Security Enforcements

The following security enforcements must be considered for the operating system environment executing any database applications:

- Database should be installed on latest supported version of the operating system with all security patches installed.
- Application recommended patches and vendor provided database patches should be installed. If not, bundled with database it should be installed separately.
- Sample default database and default users that come with database installation should be removed.
- Only Database administrators should have operating system privileges to create and delete files.
- Default installed sample procedures that comes with database installation should be removed.
- All unnecessary services and ports should be disabled at the Operating system and database level.

- LCB Finance PLC must implement information security and controls in all operating systems to a level commensurate with the sensitivity of applications and data hosted by them. This includes both server operating systems as well as workstation operating systems.
- The access rights granted in workstations and operating systems must limit the user to only the applications that are required for approved business purposes. Users must not be granted any rights to control the operating system privileges and tools.
- Users are not allowed to make alterations to the network configuration (e.g., network address, proxy settings) of any computer or any other equipment at LCB Finance. All such modifications must only be made by the Network support team or a person to whom such authority is delegated.

Install and performing OS patch updates

Regular OS patch updates

When purchasing a new PC, a compatible OS version will be installed accordingly and maintain relevant OS details in the Software Assets register. Head of IT will decide the appropriate OS version which is going to install in the relevant PC and IT delegates will make the installation process and run the approved OS updates.

When the new windows patch updates are issued, WSUS will deploy to the client PC's with the granted approval of Head of IT. In order to make approval those updates, HOIT will run the relevant KB file/s in thetest environment according to patch management process. After verifying PC event log, then HOIT will allow the relevant WSUS updated to run client PCs automatically within the LAN not before 30 days.

Server OS patch updates

Initially Server OS installed by the vendor and patch updates are maintained by the entity. According to patch, update module, Head of IT will view and verify the relevant updates and run the relevant KB file/sin the test environment according to patch management process. After verifying server event log, then HOIT will allow to run relevant, updated on the server within 30 days.

Install application software, services and protocols

Install application software

According to the applications software maintenance list maintain by the entity will be installed relevant applicable updated application to the PCs by IT delegates. Also, HOIT will deploy the compatible MS Office version with the relevant PS's according to the applications software maintenance list. MS Office updates.

In order to perform MS Office updates, HOIT will run the relevant KB file/s in the test environment according to patch management process. After verifying PC event log, then HOIT will allow the relevant WSUS updated to run client PCs automatically within the LAN not before 30 days.

Periodically review done by IT department and delegates, in order to maintain and removing unnecessary services and applications in the PCs.

Install updated Antivirus software

According to the applications software maintenance list maintain by the entity, applicable Virus Gard will be installed to the client PC's by IT delegates. Through virus guard security centre, entity will be performed monitor/upgrade/pause functions in the installed virus guard in the client PC's and automatically updates are setup to run within the day and full scan will be performed, every Friday at 12.30 p.m. or if mis task will be run following PC boot automatically.

When it is virus guard version updates, Head of IT will run the relevant application version in the test environment according to patch management process. After verifying PC event log, then HOIT will allow the relevant version updated to run client PCs and tasks will be performed by IT delegates.

Remove Unnecessary Services, Applications, and Protocols

Initially will identify what application is required for giving PCs so that a suitable level of functionality to provide, while eliminating software that is not required to improve security by regular review by IT department.

supplied defaults should not be used when performing with initial installation. Installation should be customized by regular reviewing, the entity ensures that only required packages are installed.

Creating secure accounts with required privileges

Configure users, groups and authentication

According to Access management granted the user creation procedures will create relevant useraccounts and groups within the entity and to ensure the process entity will follow the following steps:

- Restrict elevated privileges to only those users that require them
- At this stage any default accounts included as part of the system installation should be secured
- Those accounts which are not required should be either removed or at least disabled
- System accounts that manage services on the system should be set so they cannot be used for interactive logins
- Any passwords installed by default should be changed to new values with appropriate security
- Any policy that applies to authentication credentials and to password security is configured

Configure Resource Controls

Applying group policy access management granted by the entity will secure the process of configuring resource controls:

- Once the users and their associated groups are defined, appropriate permissions can be set on data and resources to match the specified policy
- This may be to limit which users can execute some programs or to limit which users can read or write data in certain directory trees

Scrutinizing all incoming and outgoing network traffic through a firewall

IT delegates will monitor the performance of firewall by regular reviewing of all the incoming and outgoing network traffic which are granted according to Firewall policy.

Test the System Security

IT delegates will check the process of initially secured base operating system in order to ensure which are taken previous security configuration and identify any possible vulnerabilities that must corrected in the process. In order to perform this, IT department will follow the software installation checklist while installation by grants IT delegates and maintain the concurrent reviewing by the other IT delegates.

Operating System Access Control

Secure Log-on Procedures

The system logon procedure shall disclose a minimum amount of information about the system. A legal banner shall appear on all LCB Finance systems prior to login on to the system. IT Department shall supplement this banner with an appropriate message. At no point in the banner or the supplement shall the system be identified by company name. Automatic terminal identification shall be used when it is important that transactions are only initiated from a specific terminal or location. The logon procedure shall not identify the system or application until the logon process has been successfully completed. The system shall validate the logon information only on completion of all input data. After a rejected logon attempt, the logon procedures must terminate.

The procedure must not explain which piece of information (the user ID or password) was the reason for the logon termination. If an error condition occurs, the system must not indicate which part of the data is correct or incorrect. The logon procedures must set a maximum time allowed for the logon process. If the time is exceeded, the system must terminate the logon process. On successful completion of logon, the logon procedures must display the date/time of the previous successful logon, and the number and date/time of unsuccessful logon attempts since the last successful logon.

Associated Procedures

System Administrators should configure the operating systems logon server to suspend the user ID after 5 consecutive unsuccessful attempts for duration of at least 1 hour. The system should be configured not to display the last username successfully accessed the system, instead logging events should record detailed information of logon activities per machine, timestamp, user name, files accessed.

Additionally, System Administrators should configure the logon procedures and controls in accordance with the policy mentioned above. On each logon, users suspecting that their systems where compromised or accessed by someone else should report immediately to the IT Department in accordance of incident management processes.

FORMS/TEMPLATES TO BE USED/REFERED

Operation System details List
Server OS details List
Application Software List
Patch updated maintain List
Software Installation Checklist

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Change Management Policy
- User Access Management

- Malware Protection
- Vulnerability Management
- Network Management & Firewall Policy

External References

- ISO / IEC 27001-(1/2)
- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment
- Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

This policy is intended to address Operating Systems Security requirements. Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or Head of IT, depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months). At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

The waiver shall be monitored to ensure its concurrence with the specified period for any exceptions.

All exceptions to this policy must be communicated through the Policy Waiver Request Form.

11. PASSWORD MANAGEMENT

PURPOSE

Passwords are the primary form of user authentication used to grant access to LCB Finance's information systems. To ensure that passwords provide as much security as possible they must be carefully created and used. Without strict usage guidelines the potential exists that passwords will be created that are easy to break thus allowing easier illicit access to LCB Finance's information systems, thereby compromising the security of those systems.

INTRODUCTION

Identification and Authentication are required elements to grant access to any protected resource. One common method to provide this is to utilize a User ID and a password. This document will provide the company accepted minimum standards for the management of User IDs and passwords. The purpose of this procedure is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

SCOPE

This document will be applicable for all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any IT facility or has access to the LCB Finance's network.

This Password Policy applies to all information systems and information system components of LCB Finance specifically, it includes:

- Systems, servers and other devices that provide centralized computing capabilities.
- SAN, NAS and other devices that provide centralized storage capabilities.
- Desktops, laptops and other devices that provide distributed computing capabilities.
- Routers, switches and other devices that provide network capabilities.
- Firewalls, IDP sensors and other devices that provide dedicated security capabilities.

OBJECTIVES

- A documented password policy is applicable and enforced for all basic user accounts in use.

DEFINITIONS

Account Lockout Threshold: This policy setting determines the number of failed sign-in attempts that will cause a user account to be locked. A locked account cannot be used until you reset it or until the number of minutes specified by the Account lockout duration policy setting expires.

Reset Account Lockout reset Counter: Reset account lockout counter after policy setting determines the number of minutes that must elapse from the time a user fails to log on before the failed logon attempt counter is reset to 0. If Account lockout threshold is set to a number greater than zero, this reset time must be less than or equal to the value of Account lockout duration.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Assistant Manager IT, IT Executive

SPECIFIC PROCEDURE

Password Security Policy

Identification and Authentication are required elements to grant access to any protected resource. One common method to provide this is to utilize a User ID and a password. This document will provide the company accepted minimum standards for the management of User IDs and passwords.

Password configurations	
Minimum Password Length	8 Characters
Enforce Password History	10 passwords remembered
Minimum Password Age	1 Day
Maximum Password Age	45 - 90 Days
Password Complexity Requirements	Enabled
Account lockout configurations	
Account Lockout threshold	5 invalid login attempts
Account Lockout Duration	1440 Minutes
Reset Account Lockout reset Counter	1440 Minutes

Password Structure

All passwords must be a minimum of eight (8) characters in length. Passwords must be difficult to guess. Words in a dictionary, common character sequences, as '1234567' must not be used. Personal details such as spouse's name, license number and birthday shall not be used unless accompanied by additional unrelated characters. Passwords must contain at least one non-alpha character. Passwords may not contain blank characters.

Summary

- The password may not contain the employee's name;
- The password must be changed at least every 60 days;
- The password must have a minimum of 8 characters;
- The password contains characters from three of the following categories:
  - 1 uppercase letter (A through Z);
  - 1 lowercase letter (a through z);
  - 1 number (0 through 9);
  - 1 special character (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- User accounts must be locked out automatically after 5 failed attempts for a period of at least 30 minutes.

11.7.3. Password Life

- All passwords should expire after a period of at least 90 days for users.
- All passwords of administrator privileges should expire after a period of 45 days
- Expired passwords should not be used for the next 10 password changes. This ensures that users do not switch between a few standard passwords at regular interval.

Invalid Logon Attempts

All systems should be set to disable user accounts in the event that there have been a maximum of three (5) consecutive invalid logon attempts. This is applicable to domain users, user id's provided to customers.

Screen Saver Policy

Password protected screen savers should be enabled and it should protect the computer/ servers within 5 minutes of user inactivity. Computers should not be left unattended with the user logged on and all screen savers should be password protected. Users should lock their computers before they leave.

Password Security

It is incumbent on all employees/ Members to do their utmost to protect their passwords. To this end, the following regulations must be followed:

- Password should not be written down under any circumstances
- Passwords are to be used and stored in a secure manner. As such, passwords are not to be written down or stored electronically. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
- Passwords are to be individually owned and kept confidential and are not to be shared under any circumstances.
- Passwords should not be divulged to any other user.
- If the password is divulged, it should be changed upon the next logon. The authorized user is responsible for all actions taken by the other party when sharing their User ID or password
- Shared/ generic accounts should have stringent controls in place on usage of those accounts. Administrators are not supposed to divulge those passwords to anyone
- Administrator passwords should be written, sealed in envelope and kept in a safe under the custody of Head of IT. In case of any emergency if the password has to be divulged it has to be approved by CEO.
- All suspected security breaches should be reported to the Head of IT and CEO to be keep informed of the incident as soon as it is noticed
- All default user accounts should be re-named, and their passwords should be changed before being exposed to the network.
- BIOS password should be enabled on all desktops and servers to prevent any unauthorized changes in BIOS.

Password Management

- The display and printing of passwords must be masked, suppressed or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them
- Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, or in other locations where unauthorized persons might discover them
- Passwords must always be encrypted when held in storage or when transmitted over networks
- Access control to files, databases, computers and other system resources via shared passwords is prohibited.

Password Distribution

- The distribution of passwords is important so that only the appropriate user has the password. It is the security administrator's responsibility to protect the password during distribution for the protection of the end user and the company.

- System administrator assigned passwords to users must be valid only for the user's first on-line session. The user must then be forced to choose another password only known to that user in order to proceed with system use.
- The distribution of each password must be handled with the highest confidentiality to ensure that only the assigned user knows the password. The user must be instructed to immediately change the password.
- Appropriate measures must be taken to confirm the identity of a user before providing passwords at any time to a use.
- Passwords may be provided by electronic means if the password is not sent in clear text.
- The password may be provided via live conversation with the intended recipient if neither party is utilizing the speaker function of their telephone system.

Specific Policy for Devices

11.1.1.1. Servers

The domain admin passwords have to meet password complexity and to be changed regularly once in every 2 months. The application admin should create login for all users providing 2 levels of authentication. The password should meet the standards as mentioned in the password policy.

11.1.1.2. Routers

The enable password and console password have to meet password complexity requirements. The passwords have to be changed regularly once in every 2 months. The Secret password has to be enabled. Telnet have to be disabled on the router and secure shell to be enabled. The SSH password has to be meet the password complexity and changed regularly once in every 2 months.

11.1.1.3. Switches

The console switch passwords have to meet the password complexity and updated regularly once in every 2 months.

11.1.1.4. Firewall and IDS

The Firewall and IDS admin password has to meet password complexity and accessed only by Secure Shell. The SSH password has to changed regularly once in every 2 months. If there is a web admin console that has to be https enabled and the password for console login should meet complexity criteria.

11.1.1.5. Databases

The database passwords have to meet password complexity requirements and to be changed regularly once in every 2 months.

Best Practices for Users

- Refrain from using your username as the password.
- Refrain from revealing the password to anyone including your superiors, IT administrators or family members.
- Do not reveal a password in an email message or over the phone.
- Refrain from talking about a password in front of others.
- Refrain hinting at the format of a password (e.g., "my family name").

- Refrain from revealing a password or details about it on questionnaires or security forms.
- If someone demands a password, refer him or her to this document or have him or her contact ~~IT Admin division.~~ Head of IT
- Password should be transmitted securely.
- Do not use the "Remember Password" feature of applications (e.g., Internet Browser Applications)
- Do not write passwords down and store them anywhere. Do not store passwords in a file on ANY computer system (including PDA's, Mobile Phones or similar devices).
- Password should be changed in regularly (ideally 45 - 90 days).
- Information users should report to the system administrator if account is locked out before 5 bad attempts. All operating system & applications should be configured to lock out the accounts after 5 bad attempts. If the account gets locked out before 5 attempts, this could be because someone else was trying to guess the password.

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- User Management Policy

External References

- ISO / IEC 27001-(1/2)

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or Director Finance , depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

12. OPERATIONS MANAGEMENT

PURPOSE & INTRODUCTION

IT Infrastructure aims at increasing system availability and ensuring smooth functioning of the system under all conditions. This covers all Hardware, Software and Network Systems. LCB Finance shall put in place clear and implementable operational procedures and change control mechanisms.

SCOPE

The Operations Management process consists of following 7 sub processes:

- Operational procedures.
- System Planning and Acceptance.
- Virus Control.
- Help Desk.
- Housekeeping.
- Network Management
- Media Handling.
- Information Exchange.

OPERATIONAL PROCEDURES

A Handbook with site-specific technical procedures to be followed is prepared and maintained in each location and is used by the infrastructure personnel. The handbook specifies the following details:

- Servers - Start up & shut down procedures, access rights and user id creation procedures and norms, maintenance & backup procedures are documented for each server.
- Software – List of software is maintained
- Network & links – Configuration details, procedures for monitoring, coordination with service providers, problem escalation, IP address management etc. are documented
- Monitoring procedures for network, server, database, power systems etc are documented
- Maintenance procedures for network, hardware, UPS etc. are documented
- Contact lists of Infrastructure personnel, vendors are maintained
- Network layout diagrams are maintained

Operational change control

Major configuration changes for critical Systems and Network assets shall undergo change management process. Asset owner shall decide the criticality of the assets. Criteria for change management process would be,

- Major configuration changes
- Major Software/Hardware upgrades
- New installations which impacts information processing facilities
- Scheduled critical maintenance

The change request records the need for change control, the impact of the proposed change, detailed change information, and contingency plan, and technical contact details. In the case of a major upgrade or change in the process Infrastructure Manager obtains approval from HOIT. Critical changes (like Latest patches installation/configuration, Firewall replacement etc) shall be communicated through e-mail to Infrastructure team.

Systems and Network Administrators are authorized to perform emergency changes upon verbal / email approval from Infrastructure Manager. Subsequent to performing such emergency changes, particulars shall be recorded as per change management process.

Sr. No	Description
1	Ownership
	The information asset owner shall be responsible for the implementation of the policy and plan the management of the asset. The Owner shall design and implement an appropriate Change Request process to ensure that change requests are evaluated, authorized, tested, documented and movement to production environment is controlled.
2	Change Request
	Any Department Head / Branch Manager or a Vendor who controls part of the Infrastructure may submit a change request to the Owner (as per the procedure defined by the owner) or the Owner may initiate a change request, specifying the following : Date and Time Name and Designation of Person Name of the Information System Asset Change Requested By Problem encountered Requested change to mitigate the problem List of document(s) attached to substantiate change The Owner shall transfer the change request details to the Change Request Form Additionally, the Owner shall specify if the requested change is recommended / not recommended
3	Change Initiation and Approval
	For a recommended change the Owner shall, after due study and evaluation, document a Change Request, which shall include the following: Change Description – a brief description of the change required Objective – the reason for making the change Affected Customers (internal, external or both) Priority – Low, High, Immediate Impact analysis - applications, end users, network segments, systems or business functions that would be affected by the change Threats – document potential failures Resource Requirement Responsibilities – personnel involved in making the change, User Acceptance Tests (before and after implementation of the change), and migrating the change to the production site Rollback Methodology Target dates - Probable Dates of testing and implementing the change in production environment. The Owner, after preparation of the above documentation, shall seek the approval of the HOIT who will evaluate the request

	For its completeness, planning, rollback plans, the timing of the change such as year end accounting etc.
4	Changes in the Change Request Form
	Once a change request is accepted, the Owner should not make any changes to the original Change Request. If a need arises to make modification to the original Change Request Form, the Owner shall inform all users involved in the process about the modifications done. The modified change request should undergo the same steps as a new change request.
5	The Change Process
	The Owner shall, with the help of the HOIT, identify the personnel who shall undertake the development of the change. The Owner shall identify personnel from the User group to carry out the User Acceptance Tests (UATs) The Owner shall submit the Change Documentation to the HOIT to carry out the change. The HOIT shall be responsible for introducing the change and maintaining all relevant documentation pertaining to the changes on the information assets.
6	Pre Implementation Process
	The Owner shall ensure that a backup of the existing system in production has been taken before implementing the change in production environment. The Owner shall review the change documentation submitted by the Head – Information Technology: Test Plans—has there been adequate testing prior to determining outcomes Assurance from the personnel responsible for the change that only the changes as specified in the Change Request Form have been initiated and that the change will not affect the functionality of other components Other dependencies—have they been completed (user training, documentation, user management etc.) Impact of the change on other scheduled / pending changes Backup of the existing system The Owner shall submit the documentation to the HOIT, who shall ensure that the documentation is complete and security of the information assets is maintained. HOIT shall submit an approval / disapproval, along with all documentation, for the implementation of the change.
7	Change Implementation Process
	On receipt of approval from the HOIT, the change is implemented ensuring that there exists a separation of duties between the personnel who developed the change to the information assets and the personnel who would be moving the changes to the production environment.
8	Post Implementation Process
	The owner shall monitor and submit a report stating the success / failure of the implementation of the change On report of a failure, the Owner shall initiate the rollback plan, if necessary. To reinitiate the change process, the Owner shall prepare a new Change Request. On report of a success, the Owner shall Maintain the modified version in the library The Owner shall inform the affected users about the implementation of the change along with training (if required) and all information (change in documentation / practice…etc.) pertaining to the change.
10	Emergency Changes
	The Owner may undertake emergency changes if necessary to recover from a system failure, hardware problems or application problems. Documentation of an emergency change shall include: Name of the user who reported the problem & the probable reason of interruption in service Name of the user who has carried out the emergency change. Date-time of the emergency change. An emergency work around until the problem is finally resolved The period of time till this workaround may be continued The risks involved in the workaround and the minimum security requirements to address these risks

System Documentation

All system documentation is stored securely and only authorized members are allowed access.

SYSTEM PLANNING AND ACCEPTANCE

Introduction

To minimize the risk of system failures system planning and acceptance is performed.

Standards and Guidelines

Advance planning and preparation are required to ensure the availability of adequate capacity and resources. The operational requirements of new systems are established, documented and tested prior to their acceptance and use.

Capacity Planning

All hardware in the organization is monitored for continuous optimal performance. This includes monitoring the performance of all hardware like Servers, Desktops, printers and other related accessories.

The primary activities done for monitoring Hardware Performance are:

- User Profile Maintenance
- Disk Space Management
- Ensuring System Data Security
- Performance Monitoring and Tuning
- Monitoring Environmental conditions

Based on the hardware monitoring activities, projections of future capacity requirements are made to ensure that adequate processing power and storage are available.

System Acceptance

Prior to acceptance of any new system, upgrades and new versions, acceptance criteria are established and tests of the new system carried out prior to acceptance.

If necessary, the new installation can be run parallel with the existing system, till the existing system is phased out. A set of manual procedures shall be prepared, where possible, which can be used when the system is not available and it becomes necessary to process any data from the application system. This may be required for critical applications. The system shall be tested for different performance / capacity requirements, keeping in consideration the production environment. Operating procedures shall be formulated and tested. User manuals shall be prepared for giving training in the operation or use of new systems.

Operating System hardening measures

Appropriate Operating system hardening measures shall be implemented for critical Windows and Unix/Linux based servers.

VIRUS CONTROL

Intoduction

Virus control software is used to prevent, detect and correct virus attacks on systems in the organization. The procedure details the process followed in maintaining and updating the virus control software.

The virus protection covers the following:

- Desktops
- Servers
- Laptops
- All incoming and outgoing S/W data in any form. Includes new software being procured.

Standards and Guidelines

- The Infrastructure manager is responsible for selection and procurement of appropriate virus control software based on the performance, cost and suitability.
- The virus control administrator shall install the latest antivirus control software in all Desktops and servers.
- Software is installed only when the virus control administrator has certified it to be virus free.
- The protection of network is done as required based on the hardware. Updates on the respective software is monitored and deployed in all servers and desktops as and when an update appears on the net. This is then recorded in a register.
- The updating the desktop/server is done automatically by pushing the update from the central console. The virus control administrator records the versions on the servers once a week. The upkeep and monitoring of the programs is done on a daily basis through a central console. Whenever a virus is detected either on Server or desktop, the virus control co-coordinator takes appropriate action to eliminate the same. The action taken to eliminate the virus is then documented in a register.
- The desktops are physically checked at random every month for effectiveness of the virus control measures and the findings documented. The Virus control Coordinator, manually updates the laptops every month and documents the same.
- All media either incoming or outgoing are scanned for virus by the virus control coordinator.
- All Desktop PC USB ports shall be disabled. Communication through e-mail is done to generate awareness regarding new viruses.

HELP DESK

Introduction

Help desk is the interface between Infrastructure team and other users. The helpdesk co-ordinates various support activities based on request from users. The helpdesk provides support in following areas:

- Backup & Restoration
- Login ID / Mail ID Creation and Deletion.
- Space Allocation
- H/W Upgrade / Maintenance
- S/W Installation/Maintenance
- Network Configuration./Maintenance
- System Change
- Uploading/Downloading data
- Virus Scanning
- Miscellaneous support during seminars, meetings, exhibition etc.

Standards and Guidelines

The activities in help desk are initiated based on the Service Request sent by the users. The activities performed under Helpdesk are categorized as:

- Service and Support
- Troubleshooting

Service and Support

The supports provided are in the form of:

- E-mail ID and Domain login Id are created for all employees who joins the organization.
- E-mail ID/domain login Ids are created based on the input given by the HR Division. Infrastructure manager shall validate and provide appropriate rights to the user. Any specific project specific login Id creation shall be requested by respective project manager User-Id request form
- User Ids shall be revoked based on the input received from the HR n Division.
- Backup & Restoration: Any specific need for backup/restoration of project related data is done on receipt of Backup and Restoration Request. This is apart from the periodic backup done by Infrastructure Team
- Space Allocation: The infrastructure team/ Infrastructure executive allocates space on the server based on the A.
- H/W, S/W Installation Upgrade / Maintenance: Initial allocation of software and hardware is done based on the resource form submitted by the HOIT. Changes to software are done on receipt of the Change Request Form.
- Network Configuration / Maintenance – Project needs on change in network configuration is done on receipt of Service request.

The engineer records the details of service done in the Call Report. The infrastructure manager reviews the reports and takes appropriate corrective action if necessary.

Trouble Shooting

The request for service for trouble shooting is sent in through appropriate Service request by the HOIT/ Department Head.

The infrastructure manager or executive- Infrastructure shall solve the problem. Records of such requests shall be maintained in a log.

HOUSEKEEPING

Introduction

The Process of backing up of data is done regularly in all servers. Presently no backup is done at the desktop level. However, the users shall have provision to store relevant data in the server, which is backed up regularly.

Standards and Guidelines

IT Executive does the backing up of all systems periodically. The periodic backup activities are of four types:

- Daily
- Weekly
- Monthly
- Yearly

All backup media are stored in fireproof cabinets at a remote site. Backup media should be tested at periodic intervals to ensure their continued availability. Back-up logs shall be stored securely.

Daily backup media are stored in onsite fireproof safe and Weekly, Monthly and Yearly backup media are stored in fireproof cabinets at a remote site.

Daily Backup

Every day, the operations staff takes a backup of all changed objects / files in each system, after all users log off. Different sets of tapes / cartridges are allocated for different days of a week. This backup is preserved for one week, after which the tapes / cartridges are recycled. A full backup is also done sometimes on need basis.

Weekly Backup

The operations staff takes Full backup of all user areas of each system on the last working day of every week.These backups are preserved for one month, after which the tapes / cartridges are recycled.

Monthly Backup

The operations staff takes backup of all system and user areas on the last working day of every month. These tapes / cartridges are preserved for a minimum period of one year.

Yearly Backup

The operations staff takes backup of all system and user areas on the working day of the last month of every year. The tapes /Cartridges are preserved for a minimum period of three years. Every tape used in the backup is provided with a unique ID. It is recommended that all tapes used for the regular backup follow the same naming convention.

Fault Logging

All faults reported by users and faults observed during back up and restoration procedures are logged into a fault log [Refer Backup Management Procedure].

NETWORK MANAGEMENT

Introduction

The purpose of Network Management is to ensure the safeguarding of information in networks.

Standards and Guidelines

The Network Management process consists of 4 sub processes as given below:

- Network Management.
- Internet Security.
- Encryption.
- E Mail Security.

Network Management

A range of controls is required to achieve and maintain security in computer networks. The Network Management activities consist mainly of:

- Installation and Configuration
- Network Administration & Monitoring
- Network Back up

Installation and Configuration:

At present there are two kinds of Network in the organization:

LAN – Local Area Network – This is used primarily for connecting the user's Desktop, Servers and other Accessories within the organization

WAN –Wide Area Network – This is used for the purpose of connecting the users of LCB Finance to other servers outside the organization and also to enable access to Internet and Intranet.

The setup of Proxy server - Firewall is done on the WAN for access to Internet and also for security and control on Internet access. The entire internal network is hidden from external networks through address translation features. The infrastructure manager tests the network for functioning and connectivity whenever a new hardware is connected to the network the Network administrator assigns the IP address for the Hardware. The Network Administrator maintains documentation of all installation and configuration done and the changes thereafter.

Network Administration & Monitoring

The main activities in Network Administration are:

Network monitoring and Link monitoring – The LAN is monitored continuously by the Network Administrator. The organization's WAN links and other project specific links are monitored on an hourly basis .The details of the links are entered into Link Monitoring Form. The details of uptime and downtime are consolidated in the form of a Link Uptime Analysis Report. WAN link is monitored using various tools. All logs shall be protected against unauthorized access and modification.

All logs pertain to network monitoring should be scrutinized by Network Administrator on a daily basis. The analysis of such logs should be reviewed by HOIT as part of the internal security audit. Any exception / vulnerability / unauthorized access, noted during such analysis should be recorded as an incident and reported to security alarm team. Troubleshooting and Support - The Network Administrator through the Help Desk support process resolves problems reported on Network.

Network Change Request - Whenever changes to network are requested the Change Request Form is used. The request records the need for change control, the impact of the proposed change, detailed change information, and contingency plan, length of the outage, and technical contact details. In the case of a major upgrade or change in the process, Infrastructure manager obtains approval from HOIT. All the change requests are tracked to closure using the Change Control.

Network Backup

The following are backed up as part of network Backup

- WAN Link
- IDS
- Firewall

INTERNET SECURITY

Introduction

To establish effective Internet security, an organization must develop controls within an information system security framework from which Internet security controls can be implemented and supported.

Standards and Guidelines

Internet

- The browsing facility is provided for carrying out the company's business and usage is subject to monitoring. Any inappropriate usage results in warnings, removal of browsing facility and other disciplinary action.
- Management reserves the right to block browsing to any select sites.
- Users are required to use the facility with responsibility and prudence, and should not carry on any objectionable, frivolous or illegal activity on the web that may damage the company's business or image.
- Web browsers are to be used in a secure manner by making use of the built in security features of the software concerned.

Security Precautions

All precautions must be taken to ensure no security risks occur. No sensitive or client-related information shall be discussed via the Internet. Be aware that any information carried over the Internet is easily susceptible to illegal access. No access or passwords are to be given out to anyone. No resources are to be made available for access from the Internet (e.g., setting up an FTP server) without explicit, written approval from Infrastructure Manager/ HOIT.

- Restrictions on Access to LCB Finance 's Network from the Internet

To protect LCB Finance's computer resources from unauthorized use, access to computer systems from the Internet is restricted except for those applications, which have been web enabled. Incoming FTP and telnet capabilities are restricted. However, the ability to access Internet hosts from a LCB Finance computer is not.

Networks Manager will provide several secure computer gateways, which will allow registered users to access LCB Finance computers from the Internet.

- Registration Policies for Systems and Users Requiring Access from the Internet

Systems allowing access from the Internet must be registered with Networks Manager, including:

- IP address
- Domain
- Administrator name and phone number
- Root password
- All user Ids and passwords

If a user requires interaction with other organizations via the Internet, and required to have that direct access to users system is needed, the users should contact LCB Finance Networks Manager.

- Security Procedures for Systems Allowing Access to LCB Finance from the Internet

Additional security procedures are in place for those systems that allow access to LCB Finance Network from the Internet. These procedures are designed to block all services that are not explicitly allowed (e.g., unauthorized access, access to unauthorized information, etc.) Following are some of the key security policies and procedures for these systems:

- Maintain system confidentiality and security by limiting access to LCB Finance information.
- Only have password entries and accounts for users that can justify their need for access from the Internet.
- Review all user accounts monthly.
- Allow no trust of any other host computer at the root level.
- Ensure system accountability via automatic logging of system access and activities.
- Log all telnet Communications protocol connections.
- Summarize and e-mail all log files to administrators.
- Track all LCB Finance users and implement appropriate procedures if the users leave the company.
- Maintain system integrity via advanced detection methods and quick restoration of system operability.
- Run intrusion detection software for all important file systems.

Internet Usage

- The Internet access available is to be used only for business purposes.

- Use or downloading of tools such as games, free software or shareware, and clip art, etc. is unauthorized. These applications pose a potential virus and security threat to system functionality and compatibility concerns, in addition to professional integrity and legal implications.

- All downloads should have authorization from Network administrator

- All kinds of Internet Chat sites such as AOL, Yahoo, MSN etc. are prohibited.

- All software, including downloaded files, must be used in accordance with the software license.

- In using the Internet, LCB Finance staff shall always maintain the highest standards of professional conduct. LCB Finance will not tolerate unprofessional use of the Internet, such as any activities related to chain letters, other solicitations, pornography, etc. Network administrator shall monitor the Internet usage, and keeps a log of every transaction done by the users.

- Any employee who violates this policy may be subject to disciplinary action, including termination.

ENCRYPTION

Introduction

Encryption is the process of converting a plaintext message into a secured form of text, called cipher text, which cannot be understood without converting back via decryption to plan text.

Standards and Guidelines

LCB Finance does not use encryption for any purpose other than to establish VPN (virtual private networks) over Internet.

E Mail Security

Introduction

Any information / data that are sensitive and / or confidential shall not be sent over E-mail without taking adequate security measures.

Standards and Guidelines

- E-Mail is the preferred medium of communication within the company All data transmitted over this network is company property
- The Email Server is a dedicated server, with no other services running on it
- The Email Server is be configured for Anti-Spamming and Anti-Relaying features
- The Infrastructure Executive monitors all email traffic. The company reserves every right to monitor, examine, block or delete any incoming or outgoing E-Mail in the company's Network
- The E-Mail facility is NOT to be used for personal gain or commercial use by any employee. Frivolous use of E-Mail for transmitting non-work related messages, pictures, jokes, programs, chain letters etc. is strictly prohibited

- The allotment of E-Mail User-IDs to employees will be made strictly on a "need to use" basis. Management reserves the right to grant / disable / revoke the User ID and access to E-mail including facilities like access to the Internet or other special features selectively at their discretion
- Every user is accountable for any mail / action that can be traced to his/her User ID. Every user has a responsibility to keep his/her password strictly confidential and is responsible for the consequences of not keeping it so
- Every employee shall take suitable protective action to prevent sending and downloading files with Viruses
- Information sent over E-Mail is essentially insecure unless special measures like encryption are taken. There fore any information / data that is sensitive and / or confidential should not be sent over E-mail
- Disciplinary action is enforced if the above steps are violated against the employee concerned ranging from warning to termination of services
- Encryption - Employees shall not encrypt data or mail with any software or mechanism that is not approved
- Standard Disclaimer shall be added automatically for all mails
- Confidential information sent by email shall be protected with password as required

MEDIA HANDLING

Introduction

Information can be stored in many forms. It could be written on papers, copied onto magnetic media such as floppy disks, hard disk drive, Tape, CD/DVD ROM, USB Stick etc. It is essential to identify these media types that can be used to hold information assets that meets Company's information security requirements and are classified appropriately. Identification of these media types also depends on the type of information assets to be stored. Information assets confidentiality, integrity and availability factors are considered while identifying media types, which hold these information assets.

Standards and Guidelines

The different media types on which information can be stored are:

- Server hard disk
- Magnetic Tape
- CD
- Floppy Diskette
- Paper
- Others

All Information stored on different media types have to be classified as per the asset classification

Server hard disk drive

Project or function specific information is stored onto respective shared folder on the server hard disk drive. This ensures that information is secure, reliable, and available to all the authorized users on the network.

Magnetic Tape

Magnetic tapes are used for information backup and archival purposes. Magnetic tapes can hold large volume of data that can be preserved for a long period, if stored as per manufacturer's specifications. Magnetic tapes can also be used for transferring large volume of data between offices or with clients.

CD / DVD

CD/DVD ROM is used to backup limited information specific to the user or project or function requirements. Original CD/DVD ROM can be copied to protect the master copy against any damage or corruption.

Request for CD/DVD copying shall be initiated by respective Department / Project managers. Project Manager shall verify the request and review the data contents before approving user's request. Upon receiving the request, Infrastructure executive shall process the request.

Paper

Information can be available on Paper media such as signed agreements, deeds and contracts, legal documents, license and warranty records, ownership documents, insurance policies, company letters, certificates, powers of attorney etc.

Others

Any other industry standard media types such as optical drives, USB storage devices etc. shall be used only on Infrastructure approval authority

Safekeeping

All storage media shall be kept at a secure place and access shall be controlled. The manufacturer's specifications pertaining to safe-keep of media and environment control shall be met. Defective media like Hard disk, CD Drive, USB drive etc, which are sent for repairs or for replacement, shall be verified and approved by authorized personnel to ensure that data is recovered and contains no information.

Non Disclosure Agreement (NDA) shall be obtained from the concerned parties where needed.

Disposal of consumables

All storage media is checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal. Damaged media where removal of data is not possible is physically destroyed.

Storage devices containing sensitive information is physically destroyed or securely overwritten
All paper documents are disposed using paper shredder. A record shall be maintained of disposal of media containing sensitive information for the purpose of audit trail. The record shall show the reason for disposal, authorization for disposal, date of disposal and manner of disposal.

INFORMATION EXCHANGE

Introduction

Controls are put in place to prevent loss modification and misuse of information that is being exchanged.

Standards and Guidelines

Information and Software exchange

In the event of any information and software exchanged between the organization and its vendors, clients, business partners, auditors, consultants it is ensured that proper security controls are implemented. Proper confidentiality and non-disclosure agreements shall be signed by the organizations prior to information / software exchange. The agreement shall mention the mode of exchange, the security issues pertaining to the same and the controls to be taken. Such controls shall include:

- Responsibilities and liabilities in the event of loss of data
- Authentication and Non-repudiation
- Encryption standard for sensitive information
- Responsibilities pertaining to safety of keys
- Responsibility for software copyright and license compliance
- Any other special control as may be agreed between the parties to agreement

Media in Transit

When sending information through postal service or via courier, reliable couriers are used. Administration maintains a list of approved couriers and these couriers are used for information exchange. Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturer's specifications. Special controls, like encryption, shall be adopted to protect sensitive information from unauthorized disclosure and modification.

13. REMOVABLE MEDIA MANAGEMENT

Introduction

LCB Finance IT will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official activities.

Purpose

This document states the Removable Media Management Policy for LCB Finance IT Services. The policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

Objectives

This policy aims to ensure that the use of removable media devices is controlled in order to:
a) Enable the correct data to be made available where it is required.
b) Maintain the integrity of the data.
c) Prevent unintended or deliberate consequences to the stability of LCB Finance computer network.
d) Avoid contravention of any legislation, policies or good practice requirements.
e) Build confidence and trust in the data that is being shared between systems.
f) Maintain high standards of care in ensuring the security of Protected and Restricted information.
g) Prohibit the disclosure of information as may be necessary by law.

Responsibility

The LCB Finance IT is responsible for ensuring that this policy is enforced and duly maintained by all staff.

Policy Ownership

Approved management responsibility for the development, review, and evaluation of the Removable Media Management Policy, for ensuring its continuing suitability, adequacy, and effectiveness is with Head of IT.

Scope

This procedure applies to all employees of the LCB Finance PLC., and contractual third parties with access to LCB Finance computer network, encompassing information, information systems or IT infrastructureas per latest IT Manual and intends to store any information on removable media devices. The scope of Removable Media Management Policy includes the protection of the confidentiality, integrity and availability of information and information processing assets.

Definitions

This procedure should be adhered to at all times, but specifically whenever any user intends to store any information used by the ~~Council~~ company to conduct official business on removable media devices. Removable media devices include, but are not limited to;

a) CDs.
b) DVDs.
c) Optical Disks.
d) External Hard Drives.
e) USB Memory Sticks (also known as pen drives or flash drives).
f) Media Card Readers.
g) Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
h) MP3 Players.
i) Digital Cameras.
j) Backup Cassettes.
k) Audio Tapes (including Dictaphones and Answering Machines).

Addressing Risks

LCB Finance IT Department recognizes that there are risks associated with users accessing and handling information for official purposes and in order to conduct the business. Information is used throughout the corporate network and sometimes shared with external organizations and applicants. Securing Confidential or Strictly Confidential data is of paramount importance – particularly in relation to the LCB Finance andIT Services need to protect data in line with the requirements of legislation of the Government of Sri Lanka.

Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of LCB Finance. It is therefore essential for the continued operation of the LCB Finance Business, the Confidentiality, Integrity and Availability of all information recording systems are maintained at a level, which is appropriate to the LCB Finance needs.

This policy aims to mitigate the following risks:

a) Disclosure of Confidential and Strictly Confidential information as a consequence of loss, theft or careless use of removable media devices.
b) Contamination of computer networks or equipment through the introduction of viruses through the transfer of data from one form of IT infrastructure to another.
c) Potential sanctions against the LCB Finance or individuals imposed by the Judiciary of Sri Lanka or other countries of operation as a result of information loss or misuse information.
d) Potential legal action against the LCB Finance or individuals as a result of information loss or misuse.
e) Reputational damage to LCB Finance as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the LCB Finance and/or LCB Finance IT and may result in financial loss and an inability to provide necessary services to our customers.

Applying the Policy

Restricted Access to Removable Media

It is LCB Finance IT policy to prohibit the use of all removable media devices, unless otherwise the use of removable devices is an authorized business requirement. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to LCB Finance IT ~~Services~~ Department. Approval for their use must be given by respective Section/Department/Division Managers.

Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased and installed by LCB Finance IT Department. Henceforth it will be an asset owned by LCB Finance.

Removable media devices must not be used to store any information used to conduct official business in LCB Finance , and must not be used with any IT equipment other than that is owned or leased by LCB Finance . The only equipment and media that should be used to connect to equipment or the corporate network is equipment and media that has been purchased by the LCB Finance and approved or has been sanctioned for use by respective Section/Department/Division
Managers.

Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up. Therefore removable media should not be the only place where data obtained for business purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer (that is backed up) until the data is successfully transferred to another networked computer or system.

In order to minimize physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment. Each user is responsible for the appropriateuse and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media devices must be protected and treated with appropriate care and attention. Where possible, such devices should be encrypted. Alternatively, all devices and/or devices holding or processing information and/or classified Confidential or Strictly Confidential is recommended to be encrypted as a data protection and leakage prevention measure.

Further information on classification can be found in Information Classification and Handling Policy. Users should be aware that IT Services of LCB Finance may audit / log the transfer of data files to and from all removable media devices and LCB Finance -owned IT equipment.

Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to IT ~~Services~~ Department as referenced in the Information Security Incident Management Policy. For further information please refer to the Information Security Incident Management Policy.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to the IT Services Manager as referenced in the Incident Management Policy & Procedure.

Third Party Access to Information

No third party (external contractors, partners, agents, and the public or non-employee parties) may receive data or extract information from the corporate network, information stores or IT equipment without explicit agreement from the LCB Finance IT.

Should third parties be allowed access to LCB Finance information then all the considerations of this policy apply to their storing and transferring of the data.

Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the IT ~~Services~~ Department should removable media be damaged. Virus and malware checking software approved by the LCB Finance IT must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned at each stage for viruses, malware etc. before information is downloaded or uploaded to and from the media.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to LCB Finance, other partner organizations or individuals from the data being lost whilst in transit or storage.

Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be returned to IT ~~Services~~ Department to be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the C or for personal use, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software (such as "Kill Disk"), tools and methods as per Asset Disposal Policy.

For advice or assistance on how to thoroughly remove all data, including deleted files from removable media contact the IT Services Department.

User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

Any removable media device used in connection with C‟s IT equipment or the network or to hold information used to conduct official purposes must only be purchased and installed by LCB Finance IT.

- Any removable media device that has not been supplied by IT Services Department must not be used.
- All data stored on removable media devices must be encrypted where possible.
- Virus and malware checking software must be used when the removable media device is connected to a machine.
- Only data that is authorized and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.
- Removable media devices must not to be used for archiving or storing records as an alternative to other storage equipment.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- For advice or assistance on how to securely use removable media devices, please contact the IT ~~Services~~ Department.

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- User Management Policy

External References

- ISO / IEC 27001-(1/2)

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT /CEO depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months). At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

14. PEOPLE MANAGEMENT

PURPOSE

This publication seeks to assist organization provide direction to LCB Finance's management on how to acquire, maintain and motivate a competent workforce for creation and delivery of IT services to the business and establish security requirements to reduce the risks of human error, theft, fraud or misuse of LCB Finance's information assets and other operational facilities.

INTRODUCTION

The Human Resources Security Policy specifies the information security requirements that need to be integrated into the HR processes during recruitment, employment and termination.

SCOPE

Information security controls shall be designed and integrated into the HR processes to ensure that employees and third-party staff understand their responsibilities, are suitable for the roles they are considered for, and reduce the risk of theft, fraud or misuse of information assets.

This policy & procedure applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance. regardless of the geographic location. This document covers all Information Systems (IS) environments operated by the entity and/or contracted with a third party by LCB Finance.

All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her systems administrator, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy.

OBJECTIVES

- To ensure User management processes for Joiner, Mover, Leaver (JML process) and controls to service (de)provisioning and delegation of user accounts are aligned with HR's starting, changing or terminating employment processes are in place.
- To ensure procedures to carry out background verification checks on all candidates for employment are in place. These should be in accordance with relevant laws, regulations and ethics and proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
- To determine the adequacy of service provisioning and delegation of user accounts is initiated from the HR process.
- To determine whether procedures are in place to ensure that all employees return [LCB Finance equipment (such as mobile devices), access cards, tokens, etc.

DEFINITIONS

Not Applicable

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT Head of Human Resources
Process delegates	IT Manager. Assistant Manager -IT, IT Executive

SPECIFIC PROCEDURE

LCB Finance shall establish a formal process for recruitment, promotion and termination of IT Department employees. LCB Finance shall identify training needs of the IT Department employees and shall provide them with the required training.

Employees Recruitment and Induction

Human Resources in coordination with the IT Department shall ensure that IT Department employees' recruitment processes are in line with the overall organization's personnel policies and procedures. Human Resources shall in coordination with the IT Department ensure that appropriate pre-employment screening, interviewing and evaluation processes are in place for the hiring of technical positions.

Human Resources shall ensure that new employees are provided with the relevant induction materials for the positions they are required to fulfil.

Associated Procedures

The IT Department should provide the Human Resources with the required skills in the new recruit for the purpose of screening potential employees. In case the IT Department is in need for employees, the Head of IT should inform the Head of Human Resources with the specific skills required in the new recruit. The Human Resources should conduct preliminary interviews for potential employees in order to ensure they have the generally required skill sets for the positions they are applying for. Optionally, Psychometric Assessment centres could be utilized to examine intelligence levels, and personality attributes profile.

Subsequent to the Human Resources has preliminary interviewed potential employee(s), the Human Resources Department should select the appropriate candidates. The Human Resources Department should raise the candidate(s) information to the IT Department. Head of IT or a manager within the IT Department whom have been assigned by the Head of IT should interview and approve the technical capability of the prospect employee prior to formal hiring.

If required, depending on the sensitivity and/or criticality of the function/position to be filled, the Human Resources Department should perform background checks for the candidate(s) (P.S. This procedure must not by any means violate any local laws and should conform to the legal/regulatory requirements in the country/countries that LCB Finance operates within). It is suggested that waivers be signed by the prospect recruit to enable such background checking.

If the candidate is qualified for the position, the Head of IT should formally approve the hiring of the employee. The Head of IT and the new employee should officially sign a "Probation Contract". The

Probation Contract should be valid for a period of 09 (nine) months and should include information but not limited to:

- Probation period salary /the salary and all allowances after the probation period provided that the employee proved capable for the position.
- Position requirements, Legal aspects relating to the position and to LCB Finance.
- Working hours, Expectations from the employee through the Job description document
- Non-disclosure agreements if required.

The Human Resources Department and, if required, the IT Department should provide the new employee with proper induction/training material based on his/her expected role in the IT Department. Head of IT, or an assigned mentor, should monitor the performance of the new employee and provide proper guidance and assistance during the Probation period. If required, the IT Department should provide the new employee with training relevant to his/her role in the IT Department. If the new employee satisfies the job requirements during his/her probation period and the Manager IT, or the assigned mentor, confirms that he/she are responsible and qualified for the position, the Manager IT should request the Human Resources Department to process the employment contract.

Employees Competencies and Training

Head of IT shall periodically verify that the IT Department employees have the appropriate competencies to fulfil their required tasks. IT Department shall provide IT Department employees with periodic training. Any specific training shall be approved by the Manager IT and provided as needed.

Associated Procedures

The Head of IT should perform annual "Competency Assessment" of the IT Department's employees. The assessment should be based on, but not limited to;

- Adherence to LCB Finance and the IT Department's roles and ethical requirements
- Contribution to the achievement of the IT Department's goals and objectives
- Meeting the position's expectations
- Potential improvement areas
- Knowledge sharing and team playing skills

Based on the assessment, the Head of IT should then suggest the required trainings needed by the IT Department's employees. The employees should then be provided with relevant training as appropriate by specialized training institutes as selected by the Head of IT or a designated manager by Head of IT in IT. However, there should be an annual training schedule for all the employees within the IT Department to increase their competency and efficiency.

If in case of special training is required due to any circumstances i.e. new advanced tools, newly acquired software, changes in the requirements the Head of IT should arrange exceptional approval of such training programs. It is critical to allocate proper budget for training expenses during the annual budgeting cycle to enable the proper execution of the IT Department training plan.

Dependence upon Individuals

The Head of IT shall minimize the exposure to critical dependency on key individuals. Through knowledge capture, knowledge sharing, succession planning and staff backup arrangements. As determined by the Head of IT, the IT Department employees shall undergo periodic compulsory/mandatory leaves to facilitate detection of resource dependency implications, required segregation of duties, fraud and/or Misconduct.

Associated Procedures

The Head of IT should ensure proper/suitable avoidance of any "conflict of interest" that could leadto any Misconduct by the IT Department employees. As part of avoiding Misconduct a possible misconduct, the Head of IT should ensure the pursuit of knowledge sharing sessions and should prepare a proper employee rotation schedule for all the IT Department's employees whilst adhering to the separation of duties principle.

The Head of IT in coordination with the Human Resources Department and with consideration of employees' special vacation requirements should prepare a compulsory annual vacation schedule. Accordingly, The Head of IT in coordination with the Head of HR should enable timely processing of leave requests.

Employee Job Performance Evaluation

Periodic evaluation of IT Department employees shall be performed against laid off individual objectives that are derived from the organization's goals, established standards and specific job responsibilities. IT Department employees shall be provided relevant coaching based on performance evaluation.

Associated Procedures

The Head of IT should set the individual objectives/expectations of each position within the department Upon finalizing the objectives/expectations, the Hed of IT should ensure that all IT Department employees are aware of their respective/relevant position objectives and expectations.

Consequently, The Head of IT, or an assigned mentor, should provide proper coaching and direction for each employee within the IT Department. Upon properly implementing the prior steps, the Head of IT should conduct annual "Performance Evaluation" based on, but not limited to:

- Technical capabilities
- Interpersonal capabilities
- Team playing skills
- Knowledge sharing and transfer
- Meeting the individual objectives and expectations

Job Change or Termination

Expedient actions shall be taken regarding job changes, especially job terminations. Based on the Head of IT approval, knowledge transfer and reassignment of responsibilities shall be arranged by the relevant unit supervisors/managers within the IT department.

Associated Procedures

The IT Department should implement an "IT Processing Facilities Database" of all IT Department employees that have access to any IT processing facilities. The head of the relevant department should immediately inform the IT Department with any access changes that might be required for employees within his/her department. The IT Department should then update the IT Processing Facilities Database with the respective changes in access rights.

Prior to terminating/transferring, the Department Heads should immediately notify the Head of IT of any terminated/transferred LCB Finance employee together with the effective date of transfer/ termination.

Upon receiving termination/transfer notification the Head of IT should ensure that all access rights for terminated/transferred employee are suspended and/or disabled on par with the effective date of the job change. The Head of IT should ensure that the IT Processing Facilities Database is updated upon the said notification.

Any information asset (in any form) that has been authorized to any such terminated / transferred personnel should be immediately returned to LCB Finance IT Department upon transfer or once the businessrequirement for this authorization is obsolete. The Human Resources Department should immediately inform Head of IT about job changes or termination to prevent granting the terminated / transferred employee any access to LCB Finance information resources.

In case of terminating/transferring an employee, the Head of IT should ensure a proper handover of the employee's information assets and knowledge transfer sessions if required to be suitably conducted.

Prior to Employment

14.1.1.1. Roles and Responsibilities

All job roles and responsibilities shall be documented and inclusive of general as well as specific responsibilities for implementing or maintaining security in LCB Finance. All employees of LCB Finance shall understand their job roles and responsibilities which include responsibility for execution of a particular security process or activity and reporting security events, potential events or other security risks to LCB Finance.

Associated Procedures

The IT Department in coordination with business departments, and the Human Resources Department should ensure that security roles and responsibilities are identified and defined based on business requirements and associated information asset criticality and classification.

Once roles and responsibilities are identified, the Human Resources Department should incorporate them into job descriptions of all employees and accordingly communicate those responsibilities to all affected employees and obtain consent of understanding of the responsibilities assigned to them and the disciplinary actions associated with these responsibilities. Additionally, Security responsibilities should be included in the performance evaluation of personnel to whom significant security roles have been assigned (such as security administrators, network administrators, etc.)

14.1.1.2. Screening

Background checks shall be performed on all personnel (including temporary personnel, contract personnel or third-party users) performing sensitive or critical job roles before they are selected for the position or transferred to the position. Periodic background checks shall be conducted on all personnel who work in sensitive or critical job roles. Information provided by personnel, at the time of recruiting shall be subjected to verification procedures.

Associated Procedures

The Human Resources and Administration Department should obtain a waiver from all prospect recruits prior to LCB Finance hiring. The waiver should enable LCB Finance to perform any background and reference checking with or without prospect recruit's knowledge. Once the waiver is obtained, the Human Resources Department in coordination with the IT Department should perform due diligence checking and technical and social background of prospect recruits as applicable. Once checking is performed and it's satisfactory to LCB Finance's requirements, the Human Resources Department should pursue hiring processing in accordance with its policies and procedures.

14.1.1.3. Terms and Conditions of Employment

The terms and conditions of employment shall contain reference to this Security Policy and shall specifically clarify the following:

- The legal and information security related responsibilities of the employee, contractor or third-party user.
- Responsibilities relating to handling of information received from other companies or third parties.
- Responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or the third-party user.
- The requirement to sign a non-disclosure agreement.
- The extent and duration of the responsibilities.
- An indication of management actions in case the terms of employment is violated.

All employees, contractors and third-party users of LCB Finance. shall sign the terms and conditions of employment/engagement as an indication of acceptance.

Associated Procedures

The Legal Department in coordination with the ed of IT should ensure that all employees,contractors and third-party users sign a Non-Disclosure Agreement at time of commencement of their association with LCB Finance and subsequently on an annual basis at the beginning of each calendar year. The Non-Disclosure agreement should clearly define the penalties that the employee should facein case of not adhering to the Non-Disclosure Agreement depending upon the nature of association of the employee, contractor or the third-party user with LCB Finance, the IT Department should also assess the requirement for continuation of the terms of employment and non-disclosure for a defined period (preferably; 2 years) after the end of the employment or association with LCB Finance.

During Employment

14.1.1.4. Management Responsibilities

LCB Finance's management is responsible for, and requires its employees, contractors and third-party users to apply security in accordance with the established Information Security Policies & Procedures.

Associated Procedures

The Department Heads and IT Department should ensure that employees, contractors and third-party users are properly briefed on their information security roles and responsibilities prior to granting them access to sensitive information resources. Accordingly, the IT Department should obtain staff members' consent of understanding of roles and responsibilities and associated disciplinary actions and penalties in case of violating LCB Finance's security policies and procedures.

14.1.1.5. Information Security Awareness, Education and Training

Each employee shall be educated with regards to information security and security awareness. Additionally, LCB Finance PLC. employees whom are involved with technical security responsibilities are required to learn additional security skills that correspond to their specific job role.

Associated Procedures

The IT Department in conjunction with Department Heads should assess the need for extending awareness training to employees, contractors and third-party users as needed. Additionally, the Human Resources Department should document and maintain details of training and certifications (if any) issued during the training in each employee's profile and send copies of training evaluation and certification to the employees' departments.

Received copies by employees' departments should maintain a record for each of their employee's training and certification to help in career planning and development. Additionally, by the help of the IT department, the HR Department should maintain a comprehensive list of all employees' awareness training and certifications awarded for applicable information security functions to help in developing a detailed schedule and deadlines in coordination with business departments to conclude any pending awareness to department employees.

Disciplinary Process

The entity shall develop a formal procedure for disciplinary actions for violations of Security Policy and supplementary security policies, and LCB Finance shall take legal action against any user found to be violating the law, as per the defined procedure.

Associated Procedures

Violations identified during audit, regular monitoring and reporting of employees should be assessed by the IT Department. Based on the assessment results, the Head of IT should confirm whether a security breach has occurred and should initiate the disciplinary process with the Human Resources Department and the Legal Department if necessary, after collection of sufficient evidence for initiation of such a process. Evidence should be in compliance to the Legal Department guidelines of evidence collection and handling processes.

The disciplinary process should take into consideration factors such as the nature and the gravity of the breach and its impact on business, relevant legislation, business contracts and other factors as required whether or not this is a first or repeat offence.

Once a decision is reached, the Human Resources Department and the Legal Department should pursue disciplinary action and accommodate any documentations, warnings, employee file updates, seize of promotions, termination of employment, suits etc. that may be part of the disciplinary action.

Termination or Change of Employment

14.1.1.6. Termination Responsibilities

Responsibility for performing employment termination or change of employment lies with the Human Resources Department and associated Business Departments.

Associated Procedures

The Human Resources Department and associated Business Departments should in advance inform the IT Department of termination and transfer activities with ample time to allow proper revocation/suspension of any assigned access and privileges assigned to the subject employee. Additionally, the Human Resources Department and associated Business Departments should inform their employees of the termination effective date so no unauthorized access is rendered to the terminated employees. All terminated employees, contractors or third-party users should be reminded of any of their legal and security responsibilities which should be valid after termination of the contract.

14.1.1.7. Return of Assets

On termination of an employee, contractor or third-party user, all information systems assets issued to the concerned person/party shall be recovered with immediate effect and prior to settlement of dues and departure from the company

Associated Procedures

All user departments are required to maintain a formal record of information assets provided to contractors or third-party service providers. Upon termination of employee, contractor or third-party user the Human Resources Department in coordination with user departments andthe IT Department should ensure that all information assets are handed over by the employee, contractor or third-party user.

Accordingly, all departments are required to ensure through all means that the concerned employee no longer is in the possession of any information or records pertaining to the entity, in case of a contractor or a third-party service provider, the user department should ensure that all information or records pertaining to LCB Finance are handed back formally by the contractor or the third-party service provider.

The Finance Department should be notified to seize any payment dues to employee, contractor or third-party user until handover clearance is provided by the Human Resources Department and the IT Department.

14.1.1.8. Removal of Access Rights

On termination of an employee, contractor or third-party user:

- All information systems access shall be revoked effective the date of issuance of termination orders.
- The concerned party's physical access to LCB Finance PLC's internal facilities shall be withdrawn and restricted.
- The concerned person shall be placed under the escort of security personnel and shall be guided out from LCB Finance PLC's premises.

Associated Procedures

At termination of an employee, the Human Resources Department should immediately communicate to all the Department Heads, including the IT Department, the exact effective date from which the employee should stand terminated.

At termination of a contractor or a third-party service provider, concerned Department Heads should communicate to all other Department Heads, including the IT Department and any related third parties, the exact date with effect from which the contractor or the third-party service provider should no longer have access to any information pertaining to LCB Finance.

Accordingly, the IT Department should ensure that all logical accesses granted to the terminated employee to LCB Finance's information resources are revoked immediately and that any identification badges and access cards are returned to LCB Finance by the terminated employee/contractor/third-party service provider prior to approving their clearance.

Upon receiving the clearance from the IT Department, the Human Resources Department should process any other outstanding clearances from other departments.

Once all pending clearances are received, the Human Resources Department should authorize the final benefits of the terminated employee. Accordingly, the Finance Department should process employee benefits payment.

FORMS/TEMPLATES TO BE USED/REFERED

- User Creation Form
- User Deactivation Form
- Clearance Form
- Access Modification Form
- Compliance Form

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Password Policy
- HR Policies
- Network Management & Firewall Policy

External References

- ISO / IEC 27001-(1/2)
- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT and/or CEO, depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

15. PHYSICAL ACCESS MANAGEMENT

PURPOSE

This policy establishes guidelines to prevent unauthorized access and interference to LCB Finance's premises and information assets. It also suggests guidelines to build security controls to prevent damage from physical security threats and environmental hazards.

INTRODUCTION

The purpose of physical security is to prevent unauthorized access, damage and interference to business premises and information. The Physical and Environmental Security Policy provides direction for the development and implementation of appropriate security controls that are required to maintain the protection of Information systems and processing facilities from physical and environmental threats.

The Physical Security process consists of 5 sub processes as given below:

- Physical Access Control
- Data Center Security
- Equipment Security
- Environmental Controls
- Clear Desk and Clear Screen Policy

SCOPE

This SOP includes guidelines applies to the policy applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance regardless of the geographic location.

This Policy covers all Information Systems (IS) environments operated by the entity and/or contracted with a third party by LCB Finance.

All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her Systems Administrator, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy.

OBJECTIVES

LCB Finance shall provide adequate protection to its information systems and facilities against unauthorized physical access and environmental security measures for protection of information systems and equipment.

The objectives of the policy are to:

- Prevent unauthorized physical access, damage and interference to the Entity's premises and information
- Ensure that critical information systems are located in secure areas, protected by the defined security perimeters, with appropriate security barriers and entry controls
- Protect the information assets by implementing environmental controls to prevent damage from environmental threats
- Regularly conduct preventive maintenance of utility equipment to ensure their continual services

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any inquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Assistant Manager – IT, IT Executive Head Of Administration, Head of HRM, Head of Risk Management

SPECIFIC PROCEDURE

Physical Access Controls

Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

15.1.1.1. Standards and Guidelines

The following physical access controls are designed to protect the organization from unauthorized access.

15.1.1.2. Entry Restrictions for Visitors

All visitors are required to sign the Visitors register. Visitors should wear a visitor badge to convey that a non-employee is in the area. Identification cards are issued to all LCB Finance employees and the employees are required to visibly display the ID card as a means of physical identification inside LCB Finance premises.

15.1.1.3. Building Security and Maintenance

Personnel Security personnel monitor the premises 24 hours a day throughout the year to ensure that the premises are protected from unlawful entry.

15.1.1.4. CCTV Camera

CCTV cameras are installed and used for monitoring. The purpose of the CCTV is for monitoring and collection of visual images for the purpose of maintaining security of premises, for preventing crime and for investigating crime. The Head of IT ~~Technical Services~~ will be responsible for the management of the system while ~~with~~ Security guard responsible for the day-to-day operation.

15.1.1.5. Confidentiality and Security

All recorded information will be kept secure and available only to those who directly concerned. Recording and processing equipment will only be accessible to those directly concerned with achieving the objectives of the system.

15.1.1.6. Quality and Maintenance

Cameras and equipment will be maintained in good condition to ensure clear images are recorded. Appropriate maintenance records shall be maintained by Administration. Any fault will be reported as

soon as possible, and repairs implemented.

15.1.1.7. Retention of Records

Recordings shall be retained for a period of 90 days.

Data Center Security

The areas where critical information systems or equipment are located are defined as Secure Areas. Such areas include Data Centers & Server Rooms. The IT Division is required to identify all restricted areas and implement additional security controls to prevent intrusion and damage to these areas. Only authorized members may enter data center.

15.1.1.8. Standards and Guidelines

Head of IT shall authorize access permission to the Data Center premises. Visitors should be escorted by an authorized member.

Data Center Security requirements:

- Suitable temperature and humidity control shall be maintained within the Data Center
- Data Center shall be maintained clean and free from dust
- No food articles or beverages shall be taken into Data Center
- No combustible article should be carried into or placed in and around Data Center.
- Information processing facilities shall be physically separated from those facilities which are managed by third parties, if any
- Back-up media shall not be stored in and around the Data center
- Necessary alternative power supply in the form of UPS, Generators etc. should be available for critical information processing facilities
- No photographic, video, audio or other recording equipment shall be allowed into the Data Center, unless authorized by the Information Security Manager.
- Employees shall be made aware of the information processing facilities and the related activities in the Data Center, only on a need-to-know basis, upon proper authorization.
- Fire extinguishers, capable of extinguishing all types of fire, should be available within the Data Center

15.1.1.9. Equipment Security

All equipment is physically protected to reduce the risks from environmental hazards and security threats. The following controls are used to protect equipment;

15.1.1.10. UPS

An Uninterruptible Power Supply is installed to ensure the continuity of services during power failure. The UPS units shall have sufficient backup to withstand till the alternative power supply is arranged. Where it is required to maintain additional secured level of uninterrupted power supply, for equipment such as severs, links etc., relevant power supply from the other UPS unit is provided. The UPS shall be maintained in a secure area, covered under regular maintenance and tested periodically in accordance with the manufacturer's instructions.

15.1.1.11. Generators

Power generators are used where necessary to ensure the continuity of services during power outages. Generators shall be maintained in a secure area, covered under regular maintenance and tested

periodically in accordance with the manufacturer's instructions. Adequate supply of fuel should always be available to ensure that the generator can perform for a prolonged period if required.

15.1.1.12. Cabling Security

Network cabling is installed and maintained by qualified engineers to ensure the integrity of both the cabling and the wall-mounted sockets.

15.1.1.13. Equipment maintenance

Authorized support providers shall maintain critical assets as per annual maintenance contract (AMC). Planned maintenance shall be carried out as per schedule and for agreed parameters as per contract.

Preventive maintenance checks shall be carried out and recorded. Break Down calls shall be recorded and communicated to the appropriate service provider. It is ensured that genuine spares are used for replacement, wherever required.

15.1.1.14. Power Distribution and Cabling

Distribution: Electrical power is distributed to the equipment through control panels, distributing panels and cabling. The layout is done in such a way that adequate size of cables for power, data, voice, audio and video are used. The cables are protected against mechanical damages. They are adequately insulated and separated to minimize the interference of signals.

Inspection: The layout drawings for the entire installation is prepared by an authorized agency and checked by the statutory body and approved by them, prior to installing the equipment. The installation is carried out by an authorized contractor. The installation is checked on installation and subsequently every year, by the Electrical Inspectorate. Deviation, if any, is reported in the Inspection Report, which shall be carried out by authorized contractor and submitted subsequently for approval by electrical inspectorate.

Power Supplies: The following fluctuations in power supply are adequately taken care of:

- Power interruption
- Voltage variation
- Frequency variation
- Earth leakage
- Power factor correction
- Short circuit protection
- Low voltage protection

Disposal of Equipment

The Obsolete equipment shall be kept in identified secure areas. The floppy / CD / tapes are checked prior to disposal. Hard disk will be low level formatted and no data in any form will be sent out.

The HODs of all Divisions are to ensure that all utility equipment, information systems, storage devices and/or Software of LCB Finance are removed from the premises of the organization with proper authorization in accordance with standard procedures.

Usage of equipment outside office premises

Necessary authorization/approvals are to be obtained from Head of IT for usage of any equipment outside office premises. The following controls shall apply to usage of equipment outside office

premises and shall be strictly observed by the person authorized to use the equipment off-premises:

- Equipment and media taken off the premises shall not be left unattended in public places.
- Manufacturer's instructions for protecting equipment shall be observed at all times
- Suitable care shall be taken while loading and off-loading such equipment / media
- The equipment / media shall be protected against theft / unauthorized access
- Suitable environmental controls shall be applied for safe-keep of equipment / media
- The person authorized for use of equipment outside office premises shall be responsible for the safe-keep of such equipment.

Removal of property

Equipment, information or software should not be removed, for maintenance or any other purpose, without prior authorization by Head of IT. Record shall be made of all such removal, including, the person authorized to remove, authorized by, date and time of removal and date and time of re-entry into LCB Finance 's premises.

Environmental Controls

Environmental exposures are primarily due to naturally occurring events, but with proper controls, exposures to these elements can be reduced.

Common exposures are:

- Fire
- Natural disasters
- Power failure
- Power spike
- AC failure
- Electrical shock
- Equipment failure
- Water damage occurring from broken water pipes or flooding

15.1.1.15. Standards and Guidelines

Smoke Detectors

Smoke detectors are installed at various locations to detect any possibilities of fire, which triggers the fire alarms. Entire work area is declared as "non-smoking zone".

Employees should switch off the electrical equipment before they leave the office. Employees are prohibited from bringing in fire hazardous item to the office.

Fire Alarms

Fire alarms are installed throughout the building and are tested periodically to ensure that they function effectively. Periodicity of testing will be once in three months. Periodic fire drills are held to assess the readiness of workforce and any corrections required in the evacuation process.

Fire Extinguishers

Fire extinguishers shall be installed at appropriate places throughout the building and shall be tested periodically to ensure that they function effectively. Fire extinguishers shall be capable of extinguishing all types of fires. Employees and security personnel shall be suitably trained to use these extinguishers in case of emergency.

Pest Control

Periodic pest control measures are implemented to protect office equipment from damage.

Air Conditioning

The purpose of providing air-conditioners is to;

- Protect the equipment from dust,
- Prevent over heating of the equipment
- Provide better working conditions for the people

Different types of air conditioning equipment are located at appropriate places. Air conditioning, ventilation and humidity controls are periodically checked to ensure effective functioning.

Water /Plumbing Leaks

- Building is periodically inspected for water/plumbing leaks.
- Smoking restrictions
- Smoking is prohibited inside the office premises.
- Food & Beverages
- Food articles are banned inside Data Centers. Employees are discouraged from eating or drinking near the data center rooms.

Impact of disaster in nearby premises

Fire or any other disaster in a neighboring building, should be immediately brought to the notice of ~~Administrator/Head of IT~~ Head of Administration and Head of IT who shall issue necessary instructions for safety of critical information processing facilities.

Employees should be trained to evacuate the building in an orderly manner, if necessary, after securing their equipment and other valuables. Fire drills shall be conducted as a minimum once a year.

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- IT Asset Management Policy
- Network Management & Firewall Policy

External References

- ISO / IEC 27001-(1/2)
- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as

determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department.

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT, depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

16. PROCURMENT AND VENDOR MANAGEMENT

PURPOSE

This publication seeks to assist organization by providing a document that defines the framework for procurement of all IT hardware, software, and any externally hosted systems or software for the use of LCB Finance. This standard and procedure must be used to provide a methodology to comply with applicable policies. The purpose of this policy is to help the entity establish security requirements in order to have a controlled access to the information resources of LCB Finance to ensure accuracy, confidentiality, and availability of information.

INTRODUCTION

This elaborates the procedure being adopted in the procurement process in the LCB Finance IT department when purchasing assets for the IT department. By following these steps the IT department will be able to comply with the Administration & Procurement Department policies and procedures.

SCOPE

This SOP includes guidelines applies to all User IDs and all system Users accessing LCB Finance technology resources. It is the responsibility of each system User to follow the standard.

This policy & procedure applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance. regardless of the geographic location. This document covers all Information Systems (IS) environments operated by the entity and/or contracted with a third party by LCB Finance.

All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her systems administrator, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy.

OBJECTIVES

Procurement policy defines the framework for procurement of all IT hardware, software, and any externally hosted systems or software for the use of LCB Finance.

- Desktop computers, Laptops, Servers and other related hardware items
- Communication equipment such as firewalls, routers, switches etc
- Printers and security surveillance equipment
- Software products
- Software as a service (SAAS)
- Public/Private Cloud based services
- Hosting services
- Any specific consultation services
-

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries

regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Assistant Manager – IT, IT Executive

SPECIFIC PROCEDURE

IT Department is the sole authority for placing orders for the above-mentioned items/services on behalf of the LCB Finance. However, during the procurement department should adhere to the following guidelines.

Budget availability

Sufficient budget provisions need to be available to procure equipment or services. If not obtain Board approval. Procurement approval limits are as per the Board approved Delegation of Authority.

The IT Department supposed to use industry standard best practices to set-up new hardware, software and systems.

Vendor/Product selection

When purchasing Capital Expenditure items (CAPEX) need to adhere to the below given guidelines. Obtain minimum of three quotations from vendors. If the service is rendered by only a specific vendor and having difficulties in obtaining three quotations, seek the approval of CEO justifying the reason.

Evaluate the quotations/proposal based on the technical specifications, price, warranty, vendor credibility, after sales support etc. IT department recommendation requires for selection upon the evaluation. However, if independent opinion or technical consultation is required from outside, it may be obtained as required.

Procurement values above Rs. 1,000,000 requires the recommendation of the IT steering committee.

Service agreements

Service agreements may have to signed to obtain different services to existing products.

- Service agreements to extend the warranty or to obtain services for a specific hardware or software products may signed depending on the requirement defined by the IT Department.
- Multiple quotations are not required when the service is obtained from the same supplier/vendor.

Equipment usable period

Any equipment may use until the possible usable period recommend by the IT department to maximize the return on investment. Due to technology enhancements obsolete equipment may need to dispose /replace to ensure the compatibility of systems.

In case of a warranty seize after the expiration of the warranty period, item may remove from use upon the recommendations made by the IT department.

IT Asset Disposal Approvals

Recommendation	Approval	Asset Value
Head of IT	CEO	Less than or equal to Rs. 100,000
IT Steering Committee, Head of IT	Board of Directors	More than Rs.100,00 and less than or equal to Rs. 1,000,000
CEO	Board of Directors	Above Rs.1,000,000

IT related consumables such as Printer Cartridges, Toners, DVDs, CDs, etc. are not considered as IT Assets and will be disposed once they reach the end of useful life-time. This process does not require any formalities to follow.

Repairs of IT related equipment

When it is requires to carry out repairs or services depending on the cost the service or repair, upon IT Departments recommendation and CEO approval may carry out as required.

16.1.1.1. Insurance of IT assets

All the IT related assets need to insure the safeguard the investment of assets.

Asset movements

To record the movement of assets Good Received Note (GRN), Goods Delivery Note (GDN), Gate pass need to be maintained.

Asset Labelling

All assets need to be labelled with the respective asset code and tag with supplier, warranty and support contact numbers.

Replacement and Purchase of Computer Hardware

Replacing a system or peripheral item would be considered if the repair cost to bring it to working order would exceed 25% of its replacement value.

16.1.1.2. Computer Specifications

The Management will decide new purchases needs or modification to the existing. This will be recommended by the IT Department as per the requirements which the specific machine is supposed to perform.

16.1.1.3. Notebook Specifications

The Management will decide new purchases need or modification to the existing This will be recommended by the IT Department as per the requirements for, which the specific machine is supposed to perform and with the availability of the stock and user request.

16.1.1.4. Server Specifications

This requirement should be based upon the individual application program needs running on the server

and individual department needs as recommended by the program vendors and the approval of the Head of IT.

16.1.1.5. Peripherals

This requirement should be assessed depending upon individual Department need as recommended by IT Department.

Disposal

An item would be considered for disposal if:

- The upgrading or repair cost to bring it to working order would exceed 25% of its replacement value.
- It has outlived its estimated useable lifetime
- The item is no longer capable of performing the task it is expected to or does not satisfy the minimum hardware specification recommended by software applications to be executed or can be upgraded.

Warranty conditions and maintenance arrangements - Then the item would be disposed of observing the procedures laid out for the disposal of corporate assets.

System Modifications

The useable life expectancy of a CPU is approximately 6 to 8 years and for Notebook computers approximately 4 to 6 years depending on the configuration of the system.

Existing computer hardware would be modified or upgraded if such cost is less than one-fourth the cost of replacement but due to an urgency, IT department can decide to modify any hardware item without prior approval.

Extra, or obsolete, computer hardware should be returned to the IT Department for re allocation or otheruse. IT Department could recommend reallocation of additional systems of as and when necessary to optimize their utility.

Roles and responsibilities

All Computer Hardware and peripherals in working or non-working condition will be the property of LCB Finance. The inventory includes all equipment bought from LCB Finance funds (from whatever source). IT Department has full authority to transfer any IT equipment with thin the company where necessary.

The Management of LCB Finance has overall responsibility for the implementation of this policy. The Head of Finance and Head of IT have responsibility for tracking of equipment and demarcating same as lost or stolen if applicable from the asset register;

Loss or theft of IT equipment must be reported immediately to the Head of Department, CEO and the Head of IT; All IT equipment must be returned to the relevant IT support team upon replacement, equipment redundancy (i.e. no longer required for business) or when repair needed.

Equipment holders will retain responsibility for equipment issued to them until it has been returned to

IT Services for redeployment or disposal; Equipment holders are not permitted to transfer their responsibilities to another member of the company without getting prior approval from the Management.

Fixed IT equipment must not be moved without the consultation of their support team and must inform to the IT department.

Equipment holders must present mobile assets such as laptops and other movable equipment to their IT support team for auditing at any time request.

Equipment used for home working will be normally audited remotely. If equipment does not allow this, alternative arrangements will be made.

IT equipment holders must make every effort to ensure that the equipment Inventory and licensing code marking is not damaged or destroyed whilst in their care, In the event that a above asset codes marking has been damaged or destroyed the equipment holder must contact the appropriate IT Department,immediately to arrange for a replacement marking.

Reporting

Any actual or suspected breach of the asset management policy must be reported to the Head of IT, who will take appropriate action and inform the relevant internal and external authorities.

FORMS/TEMPLATES TO BE USED/REFERED

Not Applicable

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Asset Management Policy
- Vendor Management Policy
- IT Risk and Security Policy
- Network Management & Firewall Policy

External References

- ISO / IEC 27001-(1/2)
- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT /and /or CEO, depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

17. ENCRYPTION MANAGEMENT

PURPOSE

This policy is intended to establish the requirements for the application of encryption to data and equipment as a means of protecting the confidentiality, integrity and availability of the LCB Finance's information assets. It also sets out any relevant standards which those controls must meet.

INTRODUCTION

This document provides the LCB Finance's with the information required to effectively and efficiently plan, prepare and deploy encryption solutions in order to secure Legally/Contractually Restricted Information (Sensitive Data) refer to LCB Finance. When properly implemented, encryption provides an enhanced level of assurance that the data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception.

SCOPE

This SOP includes guidelines on application of encryption to organization Information Asset Equipment and/or information categorized under LCB Finance's Information Classification. But the primary focus of the document is to provide guidance in the selection of encryption and cryptographic hashing methods for LCB Finance information, while "at rest" and "in transit". It applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance regardless of the geographic location.

OBJECTIVES

- Document and implement a key management process for creating, maintaining, protecting and controlling the use of cryptographic keys. Define and enforce encryption key management procedures (such as enforcing additional requirements for authorization to release a key after a request has been made)
- Implement a mechanism which ensures master keys are stored securely and access is restricted and logged. The use of master keys is documented and controlled in operational procedures
- Implement a procedure to enforce vendor-supported hard disk encryption on all end-user devices before assigning devices to end-users.
- Implement a mechanism which ensure that decryption keys are stored securely but remain available in case data recovery is needed.
- Implement mechanisms to encryption and cryptographic hashing of LCB Finance's information while "at rest" and "in transit".

DEFINITIONS

Encryption: The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text

Encryption Algorithm: A mathematical procedure for performing encryption on data. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form. Blowfish, AES RC4, RC5, and RC6 are examples of encryption algorithms.

Cryptography: Cryptography also allows senders and receivers to authenticate each other through the use of key pairs. There are various types of algorithms for encryption

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Assistant Manager -IT, IT Executive

SPECIFIC PROCEDURE

Data Encryption Procedures and Manuals

The value of the data that requires protection and the system storing, the data need to be considered carefully. Physical security refers to being able to control access to the system's storage media. All encryption methods detailed in these guidelines are applicable to desktop and all critical systems at LCB Finance. A defense in depth approach is recommended when evaluating and deploying encryption method. In an ideal situation, full disk encryption would be combined with file/folder encryption in order to provide two "layers" of encryption to protect data in the LCB Finance an event the first layer is compromised.

Followings must require but not limited to,

- All data containing confidential data, leaving the Trust must be encrypted to the standard practices.
- Advice and guidance on the use of encryption can be sought via the IT department.
- Data stored internally on Trust systems should not be encrypted by end users due to the risk of data loss if the cryptographic key is lost, the appropriate mechanisms for such events should be implemented by the ICT Department or System Developer.

Associated Data Encryption Procedures

17.1.1.1. AT-REST Encryption

Confidential Information at rest on computer systems owned by and located within LCB Finance's controlled spaces, devices, and networks should be protected by one or more of the following mechanisms:

- Disk/File System Encryption.
- Use of Virtual Private Networks (VPN's) and Firewalls with strict access controls that authenticate the identity of those individuals accessing the Confidential Information of LCB Finance.
- Sanitizing, redacting, and/or de-identifying the data requiring protection during storage to prevent unauthorized risk and exposure (e.g., masking or blurring).
- Supplemental compensating or complimentary security controls including complex passwords, and physical isolation/access to the data.
- Strong cryptography on authentication credentials (i.e. passwords/phrases) shall be made unreadable during transmission and storage on all information systems.
- File systems, disks, and tape drives in servers and Storage Area Network (SAN) environments are encrypted using industry standard encryption technology.
- Computer hard drives and other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure upon return for redistribution or disposal.

Hard drives that are not fully encrypted (e.g., disks that one or more un-encrypted partitions, virtual disks) but connect to encrypted USB devices, may be vulnerable to security breach from the encrypted

region to the unencrypted region. Full disk encryption avoids this problem and shall be the method of choice for user devices containing Confidential Information.

17.1.1.2. Portable Device Encryption

Portable devices (e.g. smart-phones, flash cards, SD cards, USB file storage) represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of Confidential Information are the result of stolen or lost portable computing devices. The most reliable way to prevent exposure is to avoid storing Confidential Information of LCB Finance on these devices.

As a general practice, Confidential Information shall not be copied to or stored on a portable computing device or LCB Finance owned computing device. However, in situations requiring Confidential Information to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

The following procedures shall be implemented when using portable storage:

- Hard drives of laptops, tablets, smartphones and personal digital assistants (PDAs) shall be encrypted using products and/or methods approved by IT department of LCB Finance. Unless otherwise approved by management, such devices shall have full disk encryption with pre-boot authentication.
- Devices shall not be used for the long-term storage of any Confidential Information of LCB Finance.
- All devices that belong to LCB Finance shall have proper and appropriate protection mechanisms installed including approved anti-malware/virus software, personal firewalls with unneeded services and ports turned off, and properly configured applications.
- Removable media including CD's, DVD's, USB flash drives, etc. shall not be used to store Confidential Information within the LCB Finance.

17.1.1.3. IN – TRANSIT Encryption

In-transit encryption refers to transmission of data between end-points. The intent of this is to ensure that Confidential Information transmitted between end points, across physical networks, or wirelessly is secured and encrypted in a fashion that protects LCB Finance's Confidential Information from a security breach.

The Head of IT or Assistant Manager IT shall ensure:

- Formal transfer policies, protocols, procedures, and controls are implemented to protect the transfer of information through the use of all types of communication and transmission facilities.
- Users follow LCB Finance acceptable use policies when transmitting data and take particular care when transmitting or re-transmitting Confidential Information received from outside party.
- Strong cryptography and security protocols (e.g. TLS, IPSEC, SSH, etc.) should be used to safeguard Confidential Information of LCB Finance during transmission over open public networks.

Such controls include,

- Only accepting trusted keys and certificates, protocols in use only support secure versions or configurations, and encryption strength is appropriate for the encryption methodology in use.
- Confidential Information transmitted in e-mail messages should encrypted. Any Confidential Information transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with LCB Finance must be encrypted or transmitted through an encrypted tunnel

(VPN) or point-to-point tunneling protocols (PPTP) that include current transport layer security (TLS) implementations.

- Wireless (Wi-Fi) transmissions used to access LCB Finance's computing devices or internal networks must be encrypted using current wireless security standard protocols (e.g. RADIUS, WPS private/public keys or other industry standard mechanisms).
- Encryption or an encrypted/secured channel is required when users access LCB Finance's Confidential Information remotely from a shared network, including connections from a Bluetooth device.
- Secure encrypted transfer of documents and Confidential Information over the internet uses current secure file transfer programs such as "SFTP" (FTP over SSH) and secure copy command (SCP).
- All non-console administrative access such as browser/web based management tools are encrypted using S based browser technologies using the most current security algorithm.

FORMS/TEMPLATES TO BE USED/REFERED

Not applicable

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy

External References

- ISO / IEC 27001-(1/2)

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department. Violation of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department.

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT and/or CEO,depending on the criticality. The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months). At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

18. ACCESS CONTROL AND USER MANAGEMENT

PURPOSE

This publication seeks to assist organization by providing a document of minimum standards regarding the use and management of Logical Access within the entity. This standard and procedure must be used to provide a methodology to comply with applicable policies. The purpose of this policy is to help the entity establish security requirements in order to have a controlled access to the information resources of LCB Finance to ensure accuracy, confidentiality, and availability of information.

INTRODUCTION

Identification and Authentication are required elements to grant access to any protected resource. One common method to provide this is to utilize a User ID and a password. This document will provide the company accepted minimum standards and procedures for the management of User IDs.

SCOPE

This SOP includes guidelines applies to all User IDs and all system Users accessing LCB Finance technology resources. It is the responsibility of each system User to follow the standard.

This policy & procedure applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance. regardless of the geographic location. This document covers all Information Systems (IS) environments operated by the entity and/or contracted with a third party by LCB Finance.

All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her systems administrator, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy.

OBJECTIVES

- To ensure all system-, application- and (privileged) accounts are treated as 'Identity'
- To ensure LCB Finance systems and data can only be accessed through authorized and authenticated identities
- To determine that authorization requests are controlled using the Joiner, Mover, Leaver (JML) process.
- To ensure access is granted based on the principles of ‘need to have’ and ‘least privilege’
- All authorizations are reviewed annually and adjusted immediately if required
- Administrative access is only granted on specifically created, personal user accounts
- Shared generic accounts are not used on business-critical systems and applications
- Non-personal / shared generic accounts are only used if other measures are implemented to determine the (source) end-user
- All user accounts (identities) are traceable to a physical person
- An up-to-date and complete authorization directory storing all identities is used
- A documented password policy is applicable and enforced for all basic user accounts in use

- Local accounts are only used if account control and password requirements are met. Cloud based access is always configured with multifactor authentication

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	IT Executive

SPECIFIC PROCEDURE

User Management Standards

18.1.1.1. User Management General Information

LCB Finance networks and computer systems should be protected from unauthorized access. An integral component of this protection is the consistent creation, administration, and management of Authentication processes.

Management of User IDs from creation to deletion will help assure that all access to LCB Finance technology resources is valid and approved. This standard establishes the minimum requirements for the management of User IDs:

- Each User is responsible for all activity performed with their personal User ID. Individual User IDs may not be utilized by anyone except the individuals to whom they have been issued.
- Where technically feasible, appropriate security systems should be implemented and figured to enforce this standard. Where there are technical limitations, management and procedural controls should be implemented to comply with these standards. Any exceptions to these standards should be documented and approved by the LCB Finance management.
- Before accessing LCB Finance system resources, all users should have their identity verified with a unique User ID and a confidential password. Where technically possible, each User will have the same ID for all platforms and systems they are authorized to use. User ID requests should be formally documented and approved by LCB Finance IT Manager and Chairman.
- LCB Finance IT Support Team and Chairman should approve all User IDs with special privileges
- Users should not leave their PC workstation or terminal unattended without either logging off or locking the workstation or terminal to prevent unauthorized access
- Users will have the minimum number of User IDs needed to perform their job function
- If a User has a valid business need for a second account that has equivalent or greater access requirements, then the current account on any Microsoft operating system or domain; the LCB Finance management should approve it
- Department Heads are responsible for reviewing and validating user access rights for every user at least on a bi-annual basis.

18.1.1.2. User ID Construction

- User IDs should be constructed with a particular format (Ideally the first Name and the first letter of the Surname) in compliance with the Information Security Policy

- IT-Support Team should develop standard template for the construction of such User ID's.

18.1.1.3. User Rights

- Administrative rights on the desktop are not allowed.
- User privileges (or rights) should be defined such that ordinary Users cannot gain access to, or otherwise interfere with the individual activities or data of other Users.
- Privileges should be established such that system Users are not able to modify production data in unrestricted manner. Users may only modify production data in approved predefined ways that preserve or enhance its integrity.
- Access control rights for all company-networked systems should be set. to a value which blocks access by unauthorized Users.
- Users should not be allowed to read, modify, delete, or copy a file belonging to another User without first obtaining permission from the owner of the file.
- Users will have the minimum number of connections (multiple simultaneous on-line) needed to perform their job function.

18.1.1.4. Non-Employee/ Third Party users

- All third parties needing access to LCB Finance systems should complete the applicable regional background screening process from LCB Finance Human Resource and Information Security department
- Third parties will not have privileged access to servers, network infrastructure components or Databases with "Sensitive" data without the Head of IT and Director Finance approval.

18.1.1.5. Privileged Users

- All multi User and network systems should support a special type of User ID that has broadly defined system privileges. This type of User ID will in turn enable authorized individuals to change the Security State of systems
- Special system privileges, such as the ability to examine the files of other Users, should be restricted to company employees directly responsible for systems management and/or security administration. These privileges should be granted only to those who have attended an approved systems administrator training class or have equivalent work experience
- Knowledge of the system administrator passwords and system administrator equivalent IDs should be limited to individuals requiring privileged access to do their job functions
- Use and granting of privileged IDs should be limited to necessary business activities and should be approved by the Head of the respective department and Chairman.
- The privileged ID (and other default accounts) that is provided as part of a delivered system should be disabled, renamed and have its password changed where technically possible.
- A system administrator emergency ID and password will be maintained in a sealed envelope in a secured area. If the ID is used, the password should be changed upon completion of the task and the ID and new password will be sealed and securely stored again. If the administration of a specific platform, such as Unix, cannot be effectively supported in the manner described, an alternative process should be set up to provide privileged functions in everyday situations
- Privileged User rights should be reviewed at least once in 3 months. If the need for any of the rights is questioned, the need should be justified, or it will be revoked immediately.

18.1.1.6. User ID Administration

- All activity involving User ID creations, deletions, and privilege changes should be securely logged and reflected in periodic management reports. Holders of privileged User IDs should not act in such a way

as to conceal their activities or mask their identities to prevent them from showing up in the security logs. Servers should be configured with enough capacity to log security related information.

- Human Resource Department should promptly report all significant changes in User duties or employment status to the IT Manager handling the User IDs of the affected persons.
- System privileges should be defined so that non-production staff members (internal auditors, information security administrators, programmers, computer operators, etc.) are not permitted to update production business information.
- User ID and access request documentation should be retained for auditing purposes.
- All Company information systems privileges should be promptly removed when the Information Security Department is notified that a worker no longer requires those functions to perform their job duties.
- Emergency or Nonstandard Access privileges will be granted on a temporary basis and require explanatory documentation, and appropriate management approval. Security administrators will be responsible for the timely removal of the temporary access. A record of all these exception items will be kept for Audit and Information Security Department reviews.

18.1.1.6. System production IDs

- System production User IDs include ID's assigned to internal systems rather than external Users. These include but are not limited to file transfer IDs, Daemon/ Server IDs, Production job ids, Started Task IDs, Gateway information exchange IDs. Under no circumstances is an end user's normal User ID considered a system production User ID.
- As these ID's are provided special privileges (Such as having non-expiring passwords), the construction and standards for these ID's should be strictly adhered with. Information Security Policy should be adhered strictly to manually change such non-expiry passwords periodically once in 3 months.
- Use of these ID's should be approved by LCB Finance Director-Finance/IT and Head of IT.
- Applications are not allowed to use Administrative or root User IDs.
- No application will be installed using the privileged access User IDs if that access should be maintained by the system. Applications will be installed with their own ID which will be used for identification and accountability purposes.

18.1.1.7. Audibility and Documentation Retention

- Significant security related events concerning the system use of User IDs should be securely logged.
- These logs should provide sufficient data to support audits of the effectiveness of and compliance with security standards. Examples of events that should be logged are access violation attempts, revocation of the User ID, and enabling of the User ID
- Logs containing Used ID security relevant events should be retained and such logs should be secured such that they cannot be modified and can only be read by authorized persons.

18.1.1.8. User Termination, Inactive Users and Transfers

- Management should promptly report all significant changes in User duties or employment status to the security administrators handling the User IDs of the affected persons
- A process should be in place to ensure that IDs for terminated and inactive users are immediately suspended/ revoked and then should be deleted within 90 days of termination. Documentation and retention should be done for auditing purpose
- IT Support Team should ensure that terminated employee has logged off all the applications and that the desktop has been powered off immediately after the individual no longer needs to access it
- The electronic equipment should be sanitized per the Equipment Security Policy
- The respective Department Head should inform Information Security department of any concerns or risks of damage to company resources in case of any terminated employee

- In the course of the termination, the terminating manager will determine in conjunction with Human Resources, the ongoing ownership of the terminated employee's data. All access to these files should be immediately removed pending ownership decision. No access will be provided to the individual's data or electronic messages without approval from Human Resources
- All information systems privileges should be promptly disabled at the time that a worker ceases to provide services to the Company
- Employees or contractors who have given notice of their intention to leave the employment or contract of the Company, as well as those who are aware of an impending involuntary employment termination, and who have special system privileges beyond that of a regular user should have these special system privileges immediately removed to minimize damage to Company assets.

18.1.1.9. Training or Testing Environments and User IDs

- Training or testing should not occur on a production environment or with production data.
- Individuals should utilize their defined ID for training or testing where possible.
- Data classified as 'Sensitive' should be 'Sanitized' prior to being used for testing or training.
- Training or testing IDs should be restricted to specific machines in a secured training or testing environment as applicable. Training and testing IDs shall be time restricted for regular training times for the particular system and ID.
- Access controls for the training and testing IDs should be reviewed every 6 months to ensure that only the minimum required access is allowed to the IDs.
- Training and testing IDs will be removed from the Domain Users group (or equivalent) and shall be primarily associated with an identified "Training/Testing" group for ease of identification, tracking and provisioning.
- Testing IDs will be required to be deleted after there is no longer a business for those ID's. The Department Head responsible for the testing project/area is responsible for notification Training IDs will be required to be deleted after 90 days of inactivity.
- Training IDs will be required to be deleted after 90 days of inactivity.
- Requiring a virtual LAN environment or separate segment to segregate the training or testing network from the production network.
- Forcing unique new passwords for every month of use for the training or testing IDs.

18.1.1.10. Administrative Access

Due to the increased risk posed by local administrative access to workstations, the need exists to strictly limit and monitor these requests.

- Desktop Administrative Access – Often application developers or other staff will require additional access to their own system to perform their job functions. In these circumstances, with the proper approval and monitoring, administrative access can be granted.
- Management of Administrative Access – Due to the additional risk that is imposed by the increase in privilege, administrative access will be granted only on an as needed basis, and the system should be monitored closely utilizing the approved security tools for system compliance monitoring and intrusion detection. The Director Finance should review and approve administrative access to desktops (including laptops, Virtual systems, etc.).
- Administrative access will be reviewed at least annually, to verify the access is still required to perform the individuals' current job function.
- If an individual's job function changes or they no longer require administrative access it is their Department Head responsibility to inform Chairman & Head of IT of the change in access requirement. These notifications should be sent in a timely manner.

18.1.1.11. Compliance Monitoring

- Information Security Department will perform compliance audits of this system monthly and as needed, to verify the continued integrity of the system

- System settings may not be modified except for those that are required to perform the defined and exact job function and that have been specifically approved
- The local administrator will not modify any system security settings such as local administrator account password, domain admin group access, local group policy, Anti-Virus, or shares unless instructed to by Information Security Department
- The local administrator should not take any action that would limit the visibility of the Domain Administrators or Information Security from being able to audit the system, adjust settings, deploy software or patches, or otherwise modify the system without specific prior and written approval from LCB Finance – Chairman.
- The local administrator should not uninstall or modify any software that has been deployed or configured as part of the standard image, standard maintenance process, or other deployment. This includes but is not limited to Software distribution tools, auditing tools, anti-virus software
- Any changes to the configuration in breach of LCB Finance Standards or Policies may be investigated as a Security Incident and appropriate corrective measures will be implemented as needed.

User Management Procedures

18.1.1.12. User ID Creation of Normal User

- All newly joined employees should duly fill the LCB Finance User ID Creation and Access Form provided by LCB Finance Human Resource Department at the time of joining.

  The following fields should be duly filled:
  - First Name
  - Middle Name
  - Last Name
  - Name
  - Employee ID No.
  - Contact Address
  - Phone No. (To be contacted in case of emergency)
  - Designation
  - Department
  - Department Head Name
  - Location
  - Date of Joining
  - Printer Access –Yes/No
  - Login ID –Yes/No
  - Email ID –Yes/No
  - Hardware –Desktop/Thin client/Laptop
  - Operating System –Windows XP
  - Applications to be installed
  - File Server access –<Server Name & Share)
  - Internet access required –Yes/No.

- Employee and their respective Department Head should duly sign the form
- Human Resource Department should cross verify the data and request Human Resource Head for authorization
- After the Human Resource Head signs the form, it should be sent to the Administrative Head for authorization. This would be required for the issuance of Access card for physical entry to the LCB Finance office

- After authorization from Department Head, Administrative Head and Human Resource Head, the form should be sent to the IT Manager for authorization.
- IT Manager should delegate the task of creation of User ID to the IT Support Team after signing the form.
- IT Support Team should create the User ID as per the standards discussed in this document.
- IT Support Team should send the form duly filled with the created Login ID to the IT Manager for verification and modification required if any suggested by him/her.
- Administrative Department should allocate the system resource as requested by the Department Head for the newly joined user and inform the IT Support Team.
- IT Support Team should provide the password to the User in person or by Phone with speaker button switched 'OFF'.
- User if finds his/her Login ID has any grammatical error, should report to the IT Support Team for modification or if User has made any grammatical error while filling the form should report to the Human Resource Head for correction and request IT Support Team for modification after appropriate approvals from Human Resource Manager and IT Manager.
- User should log in with the credentials as provided by the IT Support Team and change the password in compliance with the Password Policy.

18.1.1.13. User ID Creation of Privileged User

- Privileged User should fill the following extra fields as provided in the LCB Finance Privileged User ID Creation and Access Form
  - Manage Network/ Voice equipment/ Servers/ Database/ Desktops
  - Name of Network/Voice Device/Server/Database/Domain
  - Power User/Administrator/Custom Rights.

- Privileged User ID creation and access should be approved by the HOIT in addition to the authorization provided by the Human Resource Head, Administrative Head, Department Head and IT Head as in the User ID creation of Normal User before being processed by the IT Support Team
- Privileged User Id creation and access should be given as per the standards defined in this document
- Privileged User should be aware of the LCB Finance Information Security Policy and Standards and should comply to ensure data confidentiality, integrity and availability
- He/She should verify the privileges as provided by the IT Support Team and request any modifications required by mail to IT Manager for approval. IT manager after approval should forward the mail to the IT Support Team for taking action as per the request
- Privileged User should verify and acknowledge by mail to the IT Support Team and IT Manager

18.1.1.14. User Rights Privilege Modification

- User should raise a Change Request with detailed business reason for modification required in access privileges.
- User should send the Change Request form to the respective Department Head for approval by mail.
- Department head after approval should forward the mail to the IT Manager for approval.
- IT Manager should verify the business reason and may discuss directly with user if required, to clarify the business reason for providing such access. The IT Manager after verification may ask the user to modify the request if it requires lesser or an alternative solution that requires no privilege to access the resource.
- User after modifying the Change Request should send it to the IT Manager for approval and a copy of the mail should be sent to the respective Department Head.
- IT Manager should delegate the Change Request to the IT Support Team for further action if the Change Request is if it going to make no or less significant impact on the production environment.

- IT Manager should discuss the Change Request with the Chairman if it has a major significant impact on the production environment. IT Manager should send the mail to the Chairman for approval by mail.
- HOIT if find any exception to the Information Security Policy should consult the IT Admin for the risk acceptance.
- IT Admin should verify and after risk acceptance should approve the Change Request.
- After Change Request approval in both the cases (No/Less Significant Impact and major Significant Impact), IT Support team should take appropriate action as mentioned in the Change Request.
- IT Support Team should send the mail to the user for verification after change Request has been resolved.
- User if found unsatisfactory with the resolution should send the mail to the IT Support Team for further action.
- IT Support Team should verify the resolution and modify if required any and send the mail to the user for verification.
- User should verify and confirm that the resolution is satisfactory by mailing to the IT Support Team
- Change Request should be marked CLOSED by IT Support team and mail should be sent to the User with a copy to the IT Manager.
- The copy of the mail should be sent to the IT ADMIN and Chairman only if it involves Change Request with major significant impact on the production environment.
- Note: All mail communication should have the Change Request No. in the subject line from initiation to the closing of the Change Request.

18.1.1.15. User ID Disabling of Inactive Accounts

- IT Support Team should deploy auditing software to verify inactive accounts on the LCB Finance domain and critical servers once in three months.
- IT Support Team should log the inactive accounts and raise a Change Request with the business reason in detail for disabling such ID's. He/ She should send the mail with the Change Request No. to the IT Manager for approval.
- IT Manager should verify and consult with the Chairman and IT ADMIN if required before approving the Change Request.
- IT Manager may approve or ask IT Support Team to modify the Change request before sending it back to him/her for approval.
- IT Support team should disable the inactive User ID's as mentioned in the Change Request and approved by the IT Manager.
- IT Support Team should send the mail to the IT Manager confirming the change and marking the Change Request as CLOSED.
- The copy of the mail may be forwarded by IT Manager if required to the Chairman and IT ADMIN.

18.1.1.16. User ID Deletion

- User ID Deletion Form should be duly filled by the employee/contractor/Temp on his/her last day of services.
- User ID Deletion Form should be verified by the Department Head thoroughly to check if all the access details have been provided by the user.
- The Form should be duly signed by the Department Head, Human Resource Head, Administrative Head and sent to the IT Manager for authorization.
- IT Manager should approve and immediately send the form to the IT Support Team for revoking all the user access and disabling the User ID.
- If any authorization is required by the Chairman, IT Manager should send the form to him/her for approval and authorization.
- All User ID's should be deleted after 90 days of disabling his/her account.

- In case of any sudden termination of the employee/contractor/Temp, respective Department Head should immediately call the IT Manager to disable the User ID.
- IT Manager should delegate the task of disabling the User ID to IT Support Team immediately and ask for confirmation.
- IT Support Team should call the IT Manager and acknowledge the disabling of such User ID's.
- The emergency disabling of User ID due to sudden termination of user should be regularized by the Department Head by raising Change Request and assigning it to the IT Support Team.
- IT Manager after approval should request the IT Support Team to verify and close the Change Request.
- IT Support Team should mark the Change Request as CLOSED and confirm by mail to the IT Manager and Department Head.

18.1.1.17. Creation/ Disabling/ Deletion of User ID for Training or Testing Environment

- Creation of User ID for training or testing environment should be initiated by the user by raising a Change Request with detailed business reasons and sending the Change Request No. to the Department Head for approval.
- Department Head may ask the user to modify the Change Request if required any, before approving the Change Request.
- Department Head should send the approval mail with the Change Request No. to the IT Manager for approval.
- IT Manager may ask the user to modify the Change Request if found any and approve the Change Request.
- IT Manager should send the Change Request approval by mail to the IT Support Team for further action.
- IT Support Team should create the User ID in compliance with the Information Security Policy and User Management Standards.
- IT Support Team should send the mail to the User for verification
- User if finds any issues, should mail or call the It Support Team for resolution
- IT Support Team should resolve the issue and confirm by sending the mail to the user for verification
- IT Support Team should mark the Change Request as CLOSED and send mail to the User, IT Manager and Department Head confirming the same
- Department Head should raise a Change Request assigned to the IT Support Team to disable the User ID created for training/testing environment once the task is completed
- The Change request sent by the Department Head should be sent by mail to the IT manager for approval.
- IT Support Team should disable the User ID and send the mail to the Department Head and IT Manager with the Change Request marked as CLOSED.
- Disabled User ID should be deleted after 90 days of disabling the account.

18.1.1.18. Documentation

- Documentation and logging are the most critical requirement for auditing and tracking purposes
- The following procedure mentioned below should be logged for production, training/ testing environment and it should be available for retention as per the Information Security Policy for auditing:
  - User Creation (Normal & Privileged)
  - User Access Privilege modification
  - User Disable and Deletion.

Business requirement for access control

18.1.1.19. Access Control Policy

Access to information shall be specifically authorized in accordance with the entity's IT Asset Management policies and associated procedures. Access to information shall be controlled on the basis of business and security requirements, as well as the access control rules defined for each information system. These rules shall take into account the following:

- Security requirements of the business applications
- An identified business requirement for the user to have access to the information or business process ('need to know' principle).
- The user's security classification and the information security classification (IT Asset Management Policy).
- Legal and/or contractual obligation to restrict or protect access to information Assets.
- Definition of user access profiles and management of user access rights throughout LCB Finance's infrastructure.

All LCB Finance users shall be allowed to access only those critical business information assets and processes, which are required for performing their job duties.

Access to critical business information assets and activation of user accounts for contractors, consultants, temporary workers, or vendor personnel shall only be in effect when the individual is actively performing service for the entity.

Access for contractors, consultants, or vendor personnel to LCB Finance's critical business information assets shall be provided only on the basis of a contractual agreement.

This agreement will provide:

- The terms and conditions under which access is provided
- The responsibilities of the contractors, consultants or vendor personnel
- Agreement by the contractors, consultants or vendor personnel to abide by LCB Finance's Corporate Security Policy and Supplementary Information Security Policies. These instructions must include security requirements, such as the need to maintain the confidentiality of the information, requirements for distribution of the information, and procedures for destruction or return of the information following the period of access.

Associated Procedures

The information asset owners should define and document access profiles for applications and information assets and the information asset owners are responsible for classifying the potential users of each system into groups depending on their job descriptions and responsibilities and need for system access.

Once groups are identified, the information asset owners should determine and develop access profiles for each group based on:

- Job description of the users.
- The requirement for segregation of duties (e.g. The creator of a document cannot authorize the same).
- The 'need to know' access philosophy.

Additionally, the information asset owners should document each access profile on a matrix displaying:

- The resources that it provides access to (specific screens, functions, menus, menu options, reports etc that are available as a result of having access to the profile)
- The levels of access available (read only, modify, execute, print, etc.)

Assessing the risk associated with it and documenting the assessed risk in accordance with standard risk categories specified in this manual. Once the IT Department receives those profiles, Systems Administrators should create the profile in the test environment and test the profile to ensure that:

- The profile is functional across the application and other applications integrated with it (i.e. the profile works, and the concerned users should be able to perform their job functions using the profile)
- No screens, functions, menus, menu options, reports etc are available that would compromise the requirements for confidentiality and segregation of duties.

Upon completion of testing, the Internal Audit Department should perform the review of the test results, before rolling out user profiles to production environment if required.

Once all testing and auditing is concluded, The Manager IT should review and approve access profiles defined by the information asset owners.

Then information asset owners should present the profile to respective Department Heads for formal authorization and sign off along with all associated documentation

Once the IT Department receives the department head authorization, the Systems Administrators should deploy the approved profiles to production and ensure that Multiple User profiles are not provided simultaneously to a user.
The information asset owners should review approved access profiles every 6 months or as and when required to ensure their adequacy and appropriateness

The IT Department should regularly review system profiles to ensure they align with the approved access profiles.

In case of third-party access, the information asset owners should authorize access to third parties only on the basis of a contractual agreement. Accordingly, the Manager IT should approve any access provided to third parties and follow the prior steps to finalize the access deployment. All access to third party should be removed once the contractual agreement is concluded.

18.1.1.20. System Usernames and Passwords

- All systems usernames and passwords shall be securely stored, handled and distributed.
- All system usernames and passwords shall be maintained and documented separately by theirrespective owners along with their systems details, expiry scheme and assigned personnel details, and submitted to the Manager IT.
- Systems usernames and passwords creation, change, deletion, reuse and assignment to personnel history shall be controlled by the IT Department.
- Password strength and expiry shall be defined based on the related information asset(s) classification and compromise consequences “legal and financial”.

Associated Procedures

The IT Department should change all systems default usernames and passwords to match protection and strength requirements and/or disabled.

Once changes are implemented, a new document of all system usernames and passwords should be handed to the Manager IT and kept in a compartmentalized fire proof chub in premises. Another copy should be stored off LCB Finance premise for recovery purposes. In order to assure the confidentiality and the need-to-know principle, the document should be stored in a compartmentalized data safe with appropriate security measures in-premise and off-premise.

Subsequently, any changes should be authorized by the Manager IT and accordingly the usernames and passwords document and any of its copies should reflect such changes and proper history and documentation of password changes and assignments to personnel should be maintained in separate registers.

Based on the operating requirements of the systems and on the separation of duties concepts the Manager IT should communicate systems usernames and passwords to corresponding systems administrators.

Additionally, the Password should be a strong password i.e. should not be less than 14 characters long and contain random combinations of numerals, alphas, and special characters. For critical systems, password length should not be less than 12 characters long, and for highly critical systems, dual factor passwords should be used as needed and applicable (i.e. RSA token + a secret code).

Additionally, user name locking and password expiry should be defined based on the system requirements i.e. with a minimum of 90 days password expiry, the information asset classification, the criticality of the system and repercussions of compromise (i.e. username never locks, and password never expires for systems that depend on services that if username or password changes the licensing is invalidated, etc.)

18.1.1.21. User Password Management

All users shall abide by the terms and conditions regarding the usage and management of their user passwords as per LCB Finance's Password Policy.

The user then changes the password as per the password policy rules defined in the password use policy below, which the user is informed of and agrees to during joining formality; which specifies that the password confidentiality is to be maintained.

- The User should not use his/her name as the password
- Password should be changed after 90 days
- Password should contain minimum of 12 characters
- The characters that you use should contain three from the following categories

1. Minimum 1 uppercase letter (A-Z)
2. Minimum 1 lowercase letter (a-z)
3. Minimum 1 number (0-9)
4. Minimum 1 special character (eg ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

- User account will be locked out automatically after 5 failed attempts.

Associated Procedures

System administrators should configure the system to force users to change their passwords on the first-logon and every 45-90 days afterwards.

At each user account creation, the first login password should be a random password, which may be communicated to the user verbally in person

Additionally, system administrators should configure the operating system logon server to enable strong passwords only requirements, with minimum 14 characters long that should include alpha, numeric and special characters as a random combination and should prevent the username being part of the password.

18.1.1.22. Use of Network Services

The LCB Finance's network shall be protected through a perimeter firewall in order to protect it from exposure to public environment. Access to networked services like servers, printers etc. is provided to users as per the aforementioned sections above.

Head of IT shall ensure that the LCB Finance network will not be interconnected with any other data or voice network unless firewalls and other suitable and adequate protection is in place. Head of IT shall ensure that the access to the Internet is controlled, by using a firewall and by monitoring the Internet access usage logs.

Access to networking equipment is restricted only to the IT personnel, and the equipment are accessed through passwords, which are governed by the password use policy above.

FORMS/TEMPLATES TO BE USED/REFERED

User Creation Form
User Deactivation Form
Clearance Form
Access Modification Form
Compliance Form
Acceptable Computer Usage Policy

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Password Policy
- HR Policies
- Network Management & Firewall Policy

External References

- ISO / IEC 27001-(1/2)
- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or Director Finance , depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

19. OPERATING SYSTEM MANAGEMENT

PURPOSE

This document develops to assist the LCB Finance by providing a document of minimum standards, procedures and restrictions for end users who have legitimate business requirements to use of third-party services within the entity. This procedure must be used as guidelines to comply with applicable policies in order to ensure integrity, confidentiality and availability of the third-party security and related services.

INTRODUCTION

This policy is to help LCB Finance ensure effective management of vendor services by minimizing risks associated with under-performing vendors to facilitate meeting business operational targets from third party provided services shall have effective controlling and monitoring process of outsourced activities to ensure Continuity, Availability and Integrity of information, enabling LCB Finance to provide services and conduct its operations without any interruptions.

When outsourcing and partnering with third parties to handle sensitive data or business processes on behalf of the entity we need to Ensure these organizations handle our data securely and align their practices with our security policies and levels of risk tolerance. This is considered an important component of information security that must be accounted for. An assessment must be carried out to determine the below mentioned points.

- Identifying third parties that pose risk
- Categorization of those parties
- Development of the assessment methodology for the third parties
- Carrying out the assessments
- Reporting on the results

SCOPE

This SOP includes guidelines applies to all the third-party servicer and related services which are used in the LCB Finance technology resources. It is the responsibility of IT Department to follow the standard. This Policy cover all third-party and services operated by the entity and/or contracted with a third party by LCBFinance.

All personnel are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents,he/she shall consult with his/her, business or functional manager or IT Department as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy.

OBJECTIVES

- To ensure a procedure is implemented to maintain service level agreement (SLA) with third parties, cloud service providers and other vendors.
- To ensure a review procedure is implemented to periodically assess whether the third-party agreements are compliant with LCB Finance policies and standard
- To implement a procedure to review the third-party service catalogue and delivery.
- To ensure that procedures are in place to maintain cloud service agreement applicable for the

use and type of data to be stored/processed. This is in line with (inter)national laws

- To ensure procedures are in place in terms of reviewing written agreements on the disposition, deletion and recovery of data
- To implement procedures to review the cloud service catalogue and delivering
- To implement procedures to review to LCB Finance security policies and (inter)national laws and regulations, such as contractual agreements on data portability and extraction

DEFINITIONS

Third Party Security: A third party security is security given by an entity which secures the legal responsibility of a third party. If the third-party security does no longer include any non-public obligation to pay at the part of the mortgagor or charger, it is able to be handled like a constrained recourse assure in order that the liability of the mortgagor or charger is confined to the amount which may be realized upon disposal of the third-party security.

Third parties are categorized as:

- Any vendor, customer or partner whose security failure can lead to a security failure of any of your critical assets or systems
- with direct access to your critical systems like building management firms, co-location facility providers, IT contractors, and off-site backup services
- of critical dependencies such as Internet service providers, managed IT services vendors, and major software vendors
- Customers, business partners, and sub-tenants if they have network or physical access to your environment

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Assistant Manager IT, IT Executive

SPECIFIC PROCEDURE

Vendor Relationship Management

The IT Department shall ensure that all IT and related services to be provided by the outsourced party are clearly identified and the relationship with the outsourced party is managed through clearly identified points of contacts for and the outsourced party.

Associated Procedures

The Manager IT should ensure the existence of clearly defined understanding of the services between LCB Finance and the outsourced party through a well-established service level agreement contract. Additionally, the IT Department should maintain a list of all active SLA and their corresponding contact details.

Accordingly, the Assistant Manager IT should ensure that there is a documented contact list including all the involved people in the outsourced service from the vendor side and from LCB Finance side. The contactlist should clearly define, but not limited to, the following for each involved person:

- The name of the person to be contacted
- The role of the person in the arrangement
- The situation such person should be contacted at
- The persons phone number, mobile number and e-mail
- A secondary person to be contacted in case of the first person being unavailable

Additionally, the Manager IT should ensure that the vendor of the outsourced service has the same contact list and any changes should be timely updated and a new copy should be provided to all involved people within LCB Finance, the vendor and any parties that hold part of the agreement.

Contract Management

A formal contract shall be entered between LCB Finance and all third parties providing services to LCB Finance or using LCB Finance 's information systems. The services to be provided by the outsourced party shall be recovered by a sufficient Service Level Agreement (SLA).

All contractors shall be required to provide information to LCB Finance about related subcontractors and obtain LCB Finance's permission for the subcontracting, prior to initiation of work by the subcontractor.

Associated Procedures

The Legal Department in coordination with the Head of IT should be responsible for preparing, reviewing and approving the contracts between LCB Finance and all third parties providing services to LCB Finance or using LCB Finance's information systems.

Additionally, the Legal Department in coordination with the Head of IT should ensure that the contracts entered between LCB Finance and all third parties providing services to LCB Finance or using information systems include appropriate clauses prohibiting the third parties from engaging with any subcontractors without the permission of LCB Finance, represented by the Legal Department and the Head of IT.

Also, the Legal Department in coordination with the Head of IT should prepare SLA's to manage the service levels expected by the vendors. The IT Department should ensure that SLAs take into consideration, but not limited to, the following:

- Expected levels of service
- Security requirements
- Monitoring processes and requirements
- Contingency arrangements
- Other stipulations as appropriate

The levels of system availability should be decided by the IT Department in consultation with LCB Finance Business Departments on the basis of criticality of information systems for the business.

Vendor Risk Management

Non-Disclosure/Confidentiality agreements to protect LCB Finance 's information assets shall be signed by vendors, third parties, contractors and also by sub-contractors of the vendors. A formal process shall be in place to ensure that service problems are addressed, resolved and managed without affecting the quality of the service provided. LCB Finance shall reserve the right to select all outsourced party's personnel based on their technical competency and delivery capabilities.

Associated Procedures

The Legal Department in coordination with the Head of IT should ensure that the contracts between LCB Finance and all third parties providing services to LCB Finance or using LCB Finance's information systems include Non-Disclosure/Confidentiality Agreements that the vendor and all subcontractors must agree and sign on.

The Non-Disclosure/Confidentiality Agreements should clearly define the penalties that the vendor and/or the subcontractor should face in case of not adhering to the Non-Disclosure/Confidentiality Agreements. Accordingly, the IT Department should ensure the existence of suitable arrangements between LCB Finance, the vendors and subcontractors to address and resolve problems that might occur.

The problems' addressing and resolving arrangements should not by any means compromise the quality of the services provided. To ensure quality of service, the IT Department should define the criteria for the vendors and subcontractors' personnel's technical and delivery capabilities. The vendors and subcontractors should adhere to the criteria provided by LCB Finance.

Additionally, The IT Department should, if required based on the complexity, criticality and importance of the services to be provided, further review the technical and delivery capabilities of the vendors and subcontractors' personnel.

Vendor Performance Management

A process to monitor and report the performance of the outsourced party and to provide constructive feedback to optimize the services provided by the outsourced party shall be implemented if decided required by the Head of IT.

Associated Procedures

The IT Department should monitor the performance of the out sourced party contracting with LCB Finance under the SLA and take any measures to remedy failures in service delivery as applicable.

Additionally, business process owners receiving services under SLA's should report all service level delivery deviations to the IT Department and the Legal Department. The IT Department's involved project manager should report weekly to the Manager IT on the performance of the outsourced party on the project/service and key project/service milestones.

In case the service provided is not up to the standard that the SLA stated, the Head of IT should formally notify the outsourced party's project manager on the situation and an action should be taken to recover to the degree of agreed service level. Upon vendor failure to recover to the agreed SLA stated service delivery levels, the IT Department should notify the Legal Department for further action and should seek alternate sources to deliver the service with acceptable levels to LCB Finance business requirements.

Furthermore, the IT Department should monitor the vendor performance through a number of key performance indicators including, but not limited to:

- The percentage of vendors subject to monitoring
- The level of business satisfaction with effectiveness of communication from the vendor
- The percentage of significant incidents of vendor non-compliance per time period

FORMS/TEMPLATES TO BE USED/REFERED

Non Disclosure Agreements / Service Level Agreements maintained with Vendors

INTERNAL AND EXTERNAL REFERENCES

Internal References

- IT Security Policy
- IT Security and Risk Management Policy
- IT Asset Management Policy
- Network Management Policy
- Change Management Policy

External References

- ISO/IEC 27001

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment
- Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

This policy is intended to address Operating Systems Security requirements. Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT and/or CEO, depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months). At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

The waiver shall be monitored to ensure its concurrence with the specified period for any exceptions.

All exceptions to this policy must be communicated through the Policy Waiver Request Form.

20. BUSINESS CONTINUITY MANAGEMENT

PURPOSE

This publication seeks to assist organization in mitigating the risks through ensuring that appropriate level of Business Continuity Management is in place for counteracting interruptions to business activities and for protecting critical business processes, and to ensure their timely resumption by providing practical guidelines on responding to failures of information systems or disasters effectively and efficiently.

INTRODUCTION

The IT resources at LCB Finance is responsible for communicating the acceptable level of Information Security during a disaster and reviewing of acceptable during Disaster Recovery (DR) and Business Continuity drills recognizing the criticality and need of its business and understands the importance of availability of its key products, services, people supporting these products and services, supporting processes and information systems. The SOP is designed to minimize the system downtime and to protect the infrastructure & systems against threats & vulnerabilities.

SCOPE

This SOP includes guidelines on establishing an effective disaster response program, but the primary focus of the document is detecting, analyzing, prioritizing and handling incidents. It applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance regardless of the geographic location.

OBJECTIVES

- To ensure processes are in place to identify all critical business processes and map all business processes and systems
- To Assess all potential damage encountered through security incidents.
- To determine the Maximum Tolerable Downtime (MTD) for all critical systems and business processes with the business owner(s)/senior management.
- To determine the Recovery Time Objective (RTO) for all critical systems and business processes is determined with the business owner(s)/senior management.
- To ensure the Recovery Point Objective (RPO) is aligned with backup policies.
- To detail recovery strategies and response to critical incidents to ensure continuity of business.
- To ensure that the Business Continuity Plan has been tested in full and amendments are made where necessary.
- To ensure procedures are in place to test business continuity and disaster recovery plans at least annually.
- To determine that a back-up policy that meets the availability requirements (MTD, RTO and RPO).
- To ensure procedures are in place to test a full restore for all business-critical systems at least bi-annually.

DEFINITIONS

Business Impact Analysis (BIA): the process of gathering information to determine basic recovery requirements for your key business activities in the event of a crisis/disaster

Recovery Time Objective (RTO): the time from which you declare a crisis/disaster to the time that the critical business functions must be operational in order to avoid serious financial loss

Recovery Point Objective (RPO): The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure

Maximum Tolerable Downtime (MTD): defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences.

Risk Management: is the process of defining and analyzing risks, and then deciding on the appropriate course of action in order to minimize these risks, whilst still achieving business goals

Business Unit: smallest organizational unit, one carrying out one or more business operations

Damage: the cost of repairing or replacing an asset, plus any consequential cost or loss

Damage Assessment: Superficial assessment of impact, by the Business Continuity Team to decide if the Business Continuity Plan should be invoked. Full assessment of physical damage to premises by the Premises Manager to determine restoration needs

Disaster: any unwanted significant incident, which threatens personnel, buildings or the organizational structure of an organization which requires special measures to be taken to restore things back to normal

Critical Business Operations: those operations carried out at the premises for which there are compelling reasons why they should restart rapidly

Incident: an event, which may become disastrous

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT, Head of Risk Management, Head of Administration, Other Heads of Departments.
Process delegates	Assistant Manager, Manager IT, IT Executives

SPECIFIC PROCEDURE

Information Security in the Business Continuity Management Process

20.1.1.1. Management Statements

There shall be a managed process in place for developing and maintaining business continuity. The process shall include the following key elements of business continuity management:

- An understanding of the risks faced by the entity in terms of their likelihood and their impact, including an identification and prioritization of critical business processes.

- An understanding of the impact which interruptions caused by information security incidents are likely to have on the business, and establishing the business recovery objectives of information processing facilities
- Formulation and documentation of a business continuity strategy consistent with its business objectives and priorities
- Document and implement testing timeframes for the Business Continuity Plan
- Update the Business Continuity Plan to reflect changes in operational environment

20.1.1.2. Associated Procedures

The Information Security Steering Committee should ensure that a Business Continuity Management Process is in place and sufficient financial, organizational, technical, and environmental resources are identified to address the information security requirements for Business Continuity.

Additionally, the Information Security Steering Committee should consider purchase of suitable insurance, which may form part of the overall business continuity process, as well as being part of operational risk management.

The IT Department should identify all the information assets involved in critical business processes and report the required business continuity security aspects to the Information Security Steering Committee for review.

Accordingly, the Risk & Information Security Steering Committee should coordinate with all Department Heads on business continuity aspects and should ensure that security of critical information assets is not compromised during the execution of the business continuity plan.

Business Continuity and Risk Assessment

20.1.1.3. Management Statements

Development of Business Continuity Plan shall begin with identifying the risks that can cause interruptions to business processes (e.g. equipment failure, fire, etc).

Identification of risks shall be followed by an impact analysis to determine the probability and impact of such interruptions in terms of time, damage scale and recovery period.

The risk assessment shall identify, quantify, and prioritize risks against criteria and objectives relevant to the organization, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

20.1.1.4. Associated Procedures

The IT Department, with full involvement from business process owners and other business resources, should carry out a risk assessment periodically or after a major change in information systems environment followed by an impact analysis.
Depending on the results of the business continuity analysis and risk assessment, the IT Department should develop a high-level business continuity strategic plan to determine the overall approach to business continuity and provide it to the Information Security Steering Committee for review and approval.

Once approved, Department Heads should use the high-level business continuity strategic plan to devise their own department's business continuity plan.

All department plans should be provided to the Information Security Steering Committee for review, consolidation, risk mitigation strategies definition and approval.

Developing and Implementing Continuity Plans Including Information Security

20.1.1.5. Management Statements

The business continuity planning process shall cover the following:

- Identification and agreement of all responsibilities and business continuity procedures.
- Identification of the acceptable loss of information and services.
- Selection and implementation of the procedures to allow recovery and restoration of the business operations and availability of information in required timescales.
- Operating procedures to follow pending completion of recovery and restoration
- Documentation of agreed procedures and processes.
- Training of staff in the execution of the agreed emergency procedures and processes including crisis management.
- Testing and updating of the plans.

The planning process shall focus on the required business objective (e.g. restoring of services to customers in an acceptable amount of time). Consideration shall then be given to all the services and resources that will enable this to occur, including staffing and other non-computing requirements, as well as fallback arrangements for computer services.

20.1.1.6. Associated Procedures

The Information Security Steering Committee should approve the business continuity plan after consolidation of all departmental business continuity plans and provide the final plan to the Board of Directors.

Once the Business Continuity Plan is approved by the Information Security Steering Committee, it should then be reviewed and approved by the Board of Directors within 1 month.

Upon approval, the Information Security Steering Committee should ensure that the copies of the business continuity plans are stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. Other material necessary to execute the continuity plans should also be stored at the remote location.

Additionally, the Information Security Steering Committee should ensure that the copies of the business continuity plans are up-to-date and protected with the same level of security as applied at the main site and all members participating in the plans are aware and trained for the detailed execution process of their respective business continuity plan.

Once approved, Department Heads should use the high-level business continuity strategic plan to devise their own department's business continuity plan.

All department plans should be provided to the Information Security Steering Committee for review, consolidation, risk mitigation strategies definition and approval.

Business Continuity Planning Framework

20.1.1.7. Management Statements

A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

A business continuity planning framework shall cover the following:

- The conditions for activating the plans i.e. to assess the situation, which is to be involved, etc. before each plan is activated
- Emergency procedures, which describe the immediate action to be taken following an incident, which jeopardize business operations and/or human life.
- This shall include arrangements for media handling (to avoid/minimize the loss) and for effective liaison with appropriate public authorities (e.g. police, fire service and local government)
- Fallback procedures to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales.
- Procedures for the resumption of normal business operations.
- Maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan.
- Awareness and education activities that are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective.
- The responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternates shall be nominated as required. As well as contact information such as telephone numbers and addresses for those individuals.
- The critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures.

The Business Continuity Plan shall have a specific custodian.

Emergency procedures, manual fallback plans and resumption plans shall be the responsibility of the appropriate business owner.

20.1.1.8. Associated Procedures

The Information Security Steering Committee should develop a framework for Business Continuity planning and identify owners of the appropriate business resources or processes involved.

Once owners are identified, they should be informed, accordingly. Assigned owners should be responsible for executing emergency procedures, manual fallback plans, and resumption plans.

Additionally, the service providers should be responsible for fallback arrangements for alternative technical services, such as information processing and communication facilities.

Testing, Maintaining and Re-Assessing Business Continuity Plans

20.1.1.9. Management Statements

Business Continuity Plans shall be tested regularly to ensure that they are up to date and effective. A test schedule for the Business Continuity Plan shall be developed. The schedule shall indicate how and when each element of the plan would be tested.

A variety of techniques shall be used in order to provide assurance that the plan(s) will operate in real life. These shall include as applicable:

Table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions)

Simulations (particularly for training people in their post incident/crisis management roles)

Technical recovery testing (ensuring information systems can be restored effectively)

Testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site)

Tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment)

Complete rehearsals (testing that the organization, personnel, equipment, facilities, and processes can cope with interruptions)

Business Continuity Plan shall be maintained by regular reviews and updates, because of the changes to business environment. Examples of changes where updating of business continuity plans shall be considered are acquisition of new equipment, applications and upgrading of systems and changes in:

- Personnel
- Addresses or telephone numbers
- Business strategy
- Location, facilities, and resources
- Legislation
- Contractors, suppliers, and key customers
- Processes, or new or withdrawn ones Risk (operational and financial)

Procedures shall be included within the organization's change management program to ensure that business continuity matters are appropriately addressed.

20.1.1.10. Associated Procedures

The IT Department should develop a schedule for testing of the ~~business continuity plans~~ Disaster Recovery Plan and communicate these schedules accordingly. Once schedules are finalized, they should be provided to all concerned business departments one month prior to the testing drill to enable proper preparation.

Once tests are done, proper reporting of any recovery failures or inability to pursue the continuity of the test business function or process should be maintained.

Accordingly, the Information Security Steering Committee should review and assess reasons of failure and take corrective actions as applicable. The IT Department should redo testing with incorporated corrective actions until the test is fully successful. Once a test is fully successful, all its steps should be detailed and any required changes to the continuity plan should be incorporated by the IT Department and approved by the Information Security Steering Committee.

Additionally, the business process owners should regularly review business continuity plans to ensure that changes in business arrangements are reflected in the business continuity plans.

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Business Continuity Plan
- Disaster Recovery Plan

External References

- LCB Finance Risk Management Manual

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department.

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or CEO, depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

21. BACKUP MANAGEMENT

PURPOSE

This publication seeks to assist organization by providing a document that defines the framework for Backing up of all IT hardware, software, and any externally hosted systems or software for the use of LCB Finance. This standard and procedure must be used to provide a methodology to comply with applicable policies. The purpose of this policy is to help the entity establish security requirements in order to have a controlled access to the information resources of LCB Finance to ensure accuracy, confidentiality, and availability of information.

INTRODUCTION

This elaborates the procedure being adopted in the Back up process in the IT department. It addresses safeguarding information assets of LCB Finance , preventing the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster, permitting timely restoration of information and business processes, should such events occur. Also includes managing and securing backup and restoration processes and the media employed in the process.

SCOPE

This policy & procedure applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance regardless of the geographic location. This document covers all Information Systems (IS) environments operated by the entity and/or contracted with a third party by LCB Finance.

All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her systems administrator, business or functional manager as applicable for clarifications.

This policy applies to all servers and storage appliances in the entity. The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by the policy. The Backup retention periods are in contrast to retention periods defined by legal or business requirements.

This is an internal document and should only be shared with employees of LCB Finance and intended parties determined by Director Finance. The IT Department shall assist resolve any conflicts arising from this Policy.

OBJECTIVES

This policy defines the framework for Backup and Recovery Process to secure information at LCB Finance. The backup and restoration procedures define the type of backups to be performed, the periodicity or schedule of the backup, and the protection to be provided to backup media based on the criticality of the information.

The objectives of the Backup and Recovery procedure is:

- Ensure that timely backups are taken for identified systems and data;
- Ensure Integrity of the backed-up data is verified;
- Ensure that backup activity is monitored; and
- Ensure regular offsite storage of backups.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Manager IT. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

The IT Department should ensure sufficient backup medias are available and shall take overall responsibility for trust adherence to this policy and should randomly carry out restorations to ensure the accuracy of backups. The IT Department should ensure the completion of the backup process,

maintain the daily backup status and signed. Report any backup failures to the head of IT Department and investigate any reported exceptions.

Role	Designation
Process Owner	Head of IT
Process delegates	IT Executive Heads of Departments

SPECIFIC PROCEDURE

IT Department is the sole authority for placing orders for the above-mentioned items/services on behalf of the LCB Finance. However, during the ICT department should adhere to the following guidelines.

Identification of Data to be Backed Up

- The Respective System Owner will identify and elect as to which business application, operating system, configuration information and log files pertaining to the respective systems need to be backed up and the requirement is to be communicated to the System Administrator and Manager - IT.
- Backup schedule should be based on Recovery Time Objectives (RTO) & Recovery Point Objectives (RPO) for each application.
- System Administrator, Manager IT and respective system owner will decide and document the frequency of business/non-business data to be backed up, medium of backup, location of storage of the backup media, backup transfer methods, retention period for the backup, backup testing and restoration, security requirements and overall backup plan.
- Upon identification, information and systems needed to be backed up under the supervision of the Manager IT / IT Technicians (Infrastructure) will execute the backup plan. Backup and restoration testing of the LCB Finance systems and documents are performed according to the Backup Schedule & Backup Restoration Testing log.

Backup Procedure of Systems & Infrastructure

- If this backup schedule in some way interferes with a critical work process, then the affected user(s) will be notified by the IT department personal via email, so that exceptions or alternative arrangements can be made.
- Automated backup logs will be verified by the Manager IT/ IT Technician (Infrastructure) on daily basis.
- During backup execution, the backup success and failures are monitored regularly by the Manager IT/ IT Technician (Infrastructure).

- In the event of an error and backup failure, the Manager IT/ IT Technician (Infrastructure) will immediately investigate the particular backup failure and try to resolve the issue. If the IT Technician is able to resolve the issue immediately, will restart or continue backup from where it failed, and successfully complete the backup.
- If it was unable to resolve the issue immediately, the Manager IT/ IT Technician (Infrastructure) will mark the backup failure in the Backup Register, reschedule to back up again and the Backup

Schedule & Backup Register will be reviewed by the Head of IT once a month. This is in order to discuss and perform the next step; to resolve the failure. After resolving the issue, will restart or continue backup from where it failed, and successfully complete the backup.

- In case of restart or continuation of backup subsequent to a failure, the backup may run during business operations of the following day, while the system is Online, which should not interfere with the business operations of users.
- If the backup issue was unable to resolve, Manager IT/ IT Technician (Infrastructure) will contact the relevant third party via particular service provider for rectification under the supervision of ISO and raise an incident and follow it through to the resolution.
- Manager IT/ IT Technician (Infrastructure) will update the Backup Register immediately after the successful completion of the backup. Updated Backup Register is reviewed, approved and signed-off by Head of IT quarterly.

Infrastructure Devices Configurations Backup

- Updates on backups should be made before and after performing a change to the existing live configuration based on a High or Business Critical change request.
- All critical network device operating system images / Configuration file should be backed up and updated based on any new operating system image / Configuration update release from the vendor.

Backup Media and Storage

- Backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.
- Unique label will be used to identify the backup tape.
- Movement of the taken backup should be logged in Offsite backup movement register by the Manager IT/ IT Technician (Infrastructure), and monthly reviewed and approved by ISO.
- On-site and off-site backup will be maintained in safe custody. Only the authorized IT Department personnel and the ISO are allowed to access the backup storage.
- Backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site.
- In situations where confidentiality is of importance, backups should be given required protection.
- Backup Restoration
- Data will be restored from backup if:
  - Files have been corrupted, deleted or modified;
  - Information must be accessed that is located on an archived backup; and
  - Data is required for issue analysis and other business requirements.
- If a backup restoration is required, the employee will make the request through the email or Help Desk system to the Manager IT/ IT Technician (Infrastructure).
- Once the approval and authorization is granted by the Manager IT/ IT Technician (Infrastructure) will initiate the backup restoration process.
- Manager IT/ IT Technician (Infrastructure) will ensure that backup restoration is successful without errors. Then he will close the backup request, once each backup restoration is successfully performed. Progress will be forwarded to the respective requester and then sign-off by the ISO.

Restoration Testing

- Backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and

checked against the restoration time required. Restoration happens according to Backup Restoration Testing log.

- Manager IT/ IT Technician (Infrastructure) will perform data restoration testing according to restoration testing schedule which approved and reviewed by ISO monthly basis.
- All restoration tests will be performed on the test Environment. Manager IT/ IT Technician (Infrastructure) has the responsibility to ensure that the testing is completed without errors.
- On systems in which a restoration testing cannot be performed due to the absence of test environments, the risk of not performing restoration testing shall be identified in the risk assessment and accepted by the ISO.
- Access to test Environments should be disabled after restoration testing.

Monitoring of Backup

- Manager IT/ IT Technician (Infrastructure) will, daily monitor the automated backup execution procedure in order to identify backup success and failures immediately.
- Manager - IT will review the Backup Schedule and Backup Register to verify whether any errors or failures have been rectified and preventive measures have been taken appropriately. If applicable logs should be kept according to the rules and regulations imposed by the Government and other applicable regulatory bodies.
- If Required Manager IT/ IT Technician (Infrastructure) will provide a report to Chairman with a summary of the errors occurred, the reason and the action performed. Core business System backup process is executed after performing the day end function. System backups are copied to Network Attached Storage (NAS) located at Head Office and enable to synchronize the backup. Hard Drives are used to copy Weekly/Monthly/Annual backups per the below schedule:

Media Storage Label	Reuse	Occurrence	Retention

Friday Rewrite/use every Friday Weekly Until storage space available, thereafter rewrite the oldest.

Transportation and Storage of Backup Tapes

All System backups are written external tape drives. Media will be clearly labelled as per the above table and stored in a secure bank vault (off site backup) that is accessible only to IT staff. During transport or changes of media, media will not be left unattended.

Disposal of Media

Prior to retirement and disposal, IT will ensure that:

- The media no longer contains active backup images
- The media's current or former contents cannot be read or recovered by an unauthorized party.

With all backup media, IT will ensure the physical destruction of media prior to disposal.

User working data

Shared folders designated for user working file storage stored in cloud are not backed up since backup feature is bundled in to the solution. Shared folders designated for user working file storage stored in Network Attached Storage (NAS) appliance will be backed up as follows:

- Online real-time synchronization with the DR site NAS (with the Data transfer delay over the IP/VPN link) of shared user folders.

Emails : Exchange Mailbox stores:

- Backup of this is not performed since Microsoft Cloud email solution Office 365 is being used.

Back Up Verification

On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:

- To check for and correct errors.
- To monitor the duration of the backup job.
- To optimize backup performance where possible.

IT will identify problems and take corrective action to reduce any risks associated with failed backups.

Random test restores will be done in order to verify that backups have been successful. Back up Restoration should be conducted on a monthly basis and IT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

Data Recovery

In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days if the destroyed equipment has been replaced by that time.

In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.

Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration of information will be made to Head of IT Department.

Associated Procedures

The IT Department should develop and document detailed Backup and Restoration Procedures. The backup plan should include all source data with full path locators, and the target drive or media for each source data, the frequency of the backup, the tape/drive rotation schedules, tape sets, tape labels and coding structure.

Once the backup plan is finalized it should be rehearsed with the backup operator to ensure that the plan works as intended. It is of high importance to keep the coding structure of tape labels confidential

so in case of any exposure to tape, the perpetrator won't identify important tapes from the remaining tapes.

The IT Department should ensure that the Backup and Restoration Procedures meet the security requirements of business continuity plans and other security policies.

Information asset owners should authorize restoration of their business-related backups.

The Business Process Owners should ensure that the retention period for business information is determined and the archive copies meet those requirements. Additionally, the IT Department should consult the Legal Department on the legal retention requirement for various information classifications.

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Asset Management Policy
- Vendor Management Policy
- IT Risk and Security Policy
- Network Management & Firewall Policy

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

It is notable to state that System backups are not meant for the following purposes:

- Archiving data for future reference.
- Maintaining a versioned history of data.

Violations of the policies, standards and procedures of CDC will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Manager IT and/or Joint Director Finance, depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

22. REMOTE ACCESS AND SYSTEM LOGGING POLICY

PURPOSE

The purpose of this policy is to help LCB Finance define applicable policies for remote access and logging of computer and system logs.

INTRODUCTION

The Remote Access and System Logging Policy describes the establishment of Computer logs are essential to the operational management of an organization. They provide a primary mechanism for automated tracking and reporting for review, audit, and compliance functions as well as a useful mechanism for tracking changes and troubleshooting. Frequent monitoring and logging components are required to effectively assess information system controls, operations, and general security. This policy provides a set of logging policies and procedures aimed to establish baseline components across LCB Finance.

Where warranted, certain LCB internal resources may be remotely accessible for those employees who perform business from a remote location, such as home or when traveling. While measures have been taken to secure this type of connection, remote access is inherently a security risk. This policy is to define requirements for connecting to the LCB network from external devices via remote access technology. These requirements are designed to minimize the potential exposure to the LCB from unauthorized use and/or malicious attack that could result in loss of information or damage to critical applications.

SCOPE

This policy applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance. regardless of the geographic location. This Policy covers all Information Systems (IS) environments operated by LCB Finance. and/or contracted with a third party by LCB Finance. All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her systems administrator, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy. The Policy covers:

- Remote Access
- Computer and System Logging

DEFINITIONS

Remote access is the ability to securely access systems, applications or data that can normally only be accessed within the internal LCB Finance network. Remote Access to the LCB Finance resources is provided on a need basis and is considered an extension to your current work environment. It is not intended to be a replacement to the said environment.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation	Responsibility
Process Owner	Head of IT	~~Section 22~~
Process delegates	Assistant Manager – IT Manager – IT & IT Executive	
	HODs	

SPECIFIC PROCEDURE

All remote access of LCB Finance shall be centrally managed and will use appropriate security measures based on access requirements.

22.1.1. Management of Remote Access

Data management guidelines shall define requirements for connecting to the LCB network fromexternal devices via remote access technology. These requirements are designed to minimize the potential exposure to the LCB from unauthorized use and/or malicious attack that could result in loss of information or damage to critical applications.

Associated Procedures

22.1.1.1. Application Process

All employees requiring remote access for business purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs should his/her application be accepted. The Remote Access arrangement must be approved and signed by the employee's unit manager, supervisor, or department head before submission to the IT department. IT department do the final review and recommend or reject the application for remote system access.

22.1.1.2. Access Restrictions

Remote Access to Confidential data (referred to as PCI Identity Data) is restricted and can only be accessed using a secured security standard. This type of access requires additional approval by the Appropriate LCB Authority.

22.1.1.3. Requirements

It is the responsibility of all individuals with remote access privileges to ensure that their remote access device and connection is given the same security considerations as their on-site connection and LCB device. It is imperative that any remote access device/connection used to conduct LCB business be utilized appropriately, responsibly, and ethically. Therefore, the following requirementsmust be observed:

1. Regularly review all LCB Information Technology Policies for details of protecting information when accessing the LCB network via remote access methods, and acceptable use of the LCB network.
2. Employees will use secure remote access procedures. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home. Refer to the Password Policy for additional requirements. All remote access users using personal devices connected to the LCB network must maintain all required security standards on said devices including, but not limited to valid and up to date virus protection, malware protection and maintaining current OS and application security patches.
3. All remote access users using personal devices connected to the LCB network will notify the appropriate IT staff of possible infections while accessing services remotely.
4. The remote access user also agrees to immediately report to their manager and IT department any incident or suspected incidents of unauthorized access and/or disclosure of LCB resources.
5. All remote access connections must include a "time-out" system. In accordance with LCB security policies, remote access sessions will time out after a specified period of inactivity. The time-out will require the user to reconnect and re-authenticate in order to re-enter company networks.
6. The remote access user also agrees to and accepts that his or her access and/or connection to LCB networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by

external parties.

7. The remote access user also understands that there may be specific rules listed in the remote access application that must also be adhered too. These rules are specific to the application you are using to connect to the LCB network.

22.1.1.4. Support

Remote access to the LCB network is provided as an extension of your normal work environment. Remote access support is provided during Normal Business Hours. If you are using remote access to provide off-hours support and you experience issues with connectivity, you may have to travel to your office to provide said support.

22.1.2. Logging of System events

Access to LCB's network, systems and communications shall be logged and monitored to identify potential misuse of systems or information. Logging activities shall include regular monitoring of system access to prevent attempts at unauthorized access and confirm access control systems are effective. Log servers and documents shall be kept secure and only made available to personnel authorized by the Head of IT or his designee. These logs shall be kept as long as necessary or required for functional use or appropriate state regulation or law. This policy provides a set of logging policies and procedures aimed to establish baseline components across LCB Finance.

Associated Procedures

LCB's information systems (servers, workstations, firewalls, routers, switches, communications equipment, etc.) shall be monitored and logged to:

- Ensure use is authorized
- Manage, administer, and troubleshoot systems
- Protect against unauthorized access
- Verify security procedures and access
- Verify system and operational security
- Comply with LCB policies and procedures
- Detect and prevent criminal or illegal activities

The Head of IT or their designee shall implement automated audit trails for all critical systems and components.

At a minimum, these logs shall be used to reconstruct the following events:

- Individual user accesses to systems and sensitive information
- All actions taken by any individual with administrative privileges
- Access to audit trails
- Invalid logical access attempts and failures
- Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with administrative privileges
- Initialization, stopping, or pausing of the audit logs
- Creation and deletion of system level objects

22.1.2.1. UNDERLYING REQUIREMENTS

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit logging information to:

- Determine the activity that was performed
- Who or what performed the activity, including where or on what system the activity was performed (subject)
- Systems and objects involved
- When the activity was performed

- Status (such as success vs. failure), outcome, and/or result of the activity

LCB shall implement a suitable logging infrastructure and configure all critical devices, systems, and applications with logged audit trails. The Head of IT or their designee shall ensure important events and audit trails are logged. File integrity monitoring/change detection software shall review logs and issue alerts if the log data is altered.

22.1.2.2. ACTIVITIES TO BE LOGGED

Support staff shall be assigned to review and monitor the logs for systems under their control. Logs shall be reviewed on a regular and on-going basis. The frequency of review shall be determined according to the sensitivity of the information stored, the function of the system, and other system requirements as determined by the ISC.

Procedures should verify that logging is active and working properly to:

- Ensure events are properly classified
- Review logging for performance delays
- Ensure compliance related logging cannot be bypassed
- Verify access to log files is properly restricted
- Assist with investigations

Logs shall be created whenever the following activities are performed by a system, application, or user:

- Creating, reading, updating, or deleting confidential information, including confidential authentication information such as passwords
- Initiating or accepting a network connection
- Authenticating user access and security authorizations
- Granting, modifying, or revoking access rights to include new user or group additions, user privilege modifications, file or database object permissions, firewall rules, and user password changes
- Configuring systems, networks, or services for maintenance and security changes including installation of software patches and updates, or other installed software
- Changing statuses of application process startup, shutdown, and/or restart
- Application process aborts, failures, or abnormal conditions due to resource limits or thresholds (such as for CPU, memory, network bandwidth, disk space, or other key system resources), failure of network services, or hardware faults
- Detection of suspicious/malicious activity such as from an intrusion detection or prevention system, anti-virus, or anti-spyware system

22.1.2.3. SYSTEM LOG ELEMENTS

System events and activities that shall be monitored and logged are as follows:

- System administrator and system operator activities
- System start-ups and shut-downs
- Logging start-ups and shut-downs
- Backups and restorations/roll-backs
- Exceptions and security events
- Database commits and transactions
- Protection software and hardware (firewalls, routers, etc.)
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems
- Modifications to data characteristics including permissions, location, file type
- Authentication successes and failures (e.g. log in, log out, failed logins)

22.1.2.4. APPLICATION LOG ELEMENTS

Third party and custom application software logging requires more than just relying on server based

system logs. Application logs help identify security incidents, establish baselines, provide information about problems and unusual conditions, assist with incident investigation, and help detect intrusions and errors. Application events and activities that shall be monitored and logged include:

- Application authentication (e.g. successes, failures, logouts)
- Data audit trails (e.g. access to sensitive data, adding data, modifying data, deleting data, exporting and importing data)
- Input validation failures (e.g. protocol violations, unacceptable encodings, invalid parameter names and values)
- Output validation failures (e.g. database record mismatch, invalid data encoding)
- Suspicious behavior (e.g. multiple records deleted in a short period of time, invalid access attempts)
- Session management failures (e.g. cookie session identification value modifications)
- Application errors and events (e.g. syntax and runtime errors, connectivity problems, third party service error messages, file system errors, sequencing failure)
- Higher-risk functionality (e.g. adding and deleting users, changes to access privileges, use of administrative privileges, access by application administrators, and access to sensitive data)
- Legal compliance services (e.g. permissions to transfer information, terms of use, and parental consent)
- Security events or warnings

22.1.2.5. LOGGING ELEMENTS

Log entries can contain a number of elements based on the type and function of the audited system/process. Generally, automated audit trails shall include the following information:

- Host name, system component, or resource
- Date/Time Stamp
- Application ID (e.g. name and version)
- Initiating Process ID or event origination (e.g. entry point URL, page, form)
- Code location (e.g. module, subroutine)
- User initiating action (e.g. user ID)
- Event type
- Result status (e.g. success, failure, defer)
- Resource (e.g. identity or name of affected data, component)
- Location (e.g. IP address or location)
- Severity of event (e.g. emergency, alert, fatal error, warning, information only)
- Other (e.g. parameters, debug information, system error message)

22.1.2.6. FORMATTING AND STORAGE

The system shall support the formatting and storage of audit logs to ensure integrity enterprise-level analysis and reporting. Mechanisms known to support these goals include but are not limited to the following approaches:

- Collecting Microsoft Windows Event Logs from servers by a centralized logging management system
- Storing logs in a documented format and sent via reliable network protocols to a centralized log management system
- Storing log entries in a SQL database that generates audit logs in compliance with the requirements of this policy.

22.1.2.7. INFORMATION SECURITY ISSUES

Logs are one of the primary tools used by system administrators and management to detect and investigate attempted and successful unauthorized activity and to troubleshoot problems. Detailed procedures that support this policy shall be developed to protect against and limit log security risks

such as:

- Controls that limit the ability of administrators and those with operating system command line access to disable, damage, or circumvent access control and audit log mechanisms
- Protecting the contents of system logs from unauthorized access, modification, and/or deletion
- Limiting outside access to logging systems to extreme or emergency circumstances. Any emergency access should be authorized by the Partner IT and use of tools bypassing security controls should be documented
- Limiting changes to the auditing policies to stop logging of an unauthorized activity. Log settings should be set to track and record user policy changes

22.1.2.8. ADMINISTRATIVE RESPONSIBILITIES

The IT Manager shall be responsible for:

- Separating duties between operations and security monitoring
- Ensuring a regular review of activity audit logs, access reports, and security incidents
- Approving the types of logs and reports to be generated, review activities to be performed, and procedures that describe the specifics of the reviews
- Procedures that specify monitoring log-in attempts, reporting discrepancies, and processes used to monitor log-in attempts
- Procedures that specify audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems
- Procedures ensure that the audit controls meet security requirements by recording and examining activity related to sensitive information
- Securing audit trails by limiting viewing to those with a job-related need
- Protecting audit trail files from unauthorized modifications
- Ensuring audit trail files are promptly backed up to a centralized log server or media
- Audit Controls and Management
- On-demand documented procedures and evidence of practice should be in place for this operational policy as part of LCB procedures. Examples of auditable controls include:
- On demand and historical log reviews of areas described in this policy
- Documented communications surrounding logging activities
- Incident response procedures

22.2. INTERNAL AND EXTERNAL REFERENCES

22.2.1. Internal References

- Information Security Policy
- Change Management Procedures
- Asset Management Procedures
- User Management Procedure
- Network Management

22.2.2. External References

- LCB International – Framework Remediation Controls

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as

determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT and/or Partner - IT, depending on the criticality. The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

23. DATA MANAGEMENT AND CLASSIFICATION MANAGEMENT

PURPOSE

The purpose of this policy is to help LCB Finance define applicable policies for data management and classification.

INTRODUCTION

The Data Management Policy describes the establishment of a framework for classifying institutional data based on its level of sensitivity, value and criticality to the Entity as required by the Entity's Information Security Policy. Classification of data will aid in determining baseline security controls for the protection of data.

SCOPE

This policy applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance. regardless of the geographic location. This Policy covers all Information Systems (IS) environments operated by LCB Finance. and/or contracted with a third party by LCB Finance.All users are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with his/her systems administrator, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy. The Data Management and Classification Policy covers:

- Data Verification and Authorization
- Data Classification

DEFINITIONS

Confidential Data is a generalized term that typically represents data classified as Restricted, according to the data classification scheme defined in this Guideline. This term is often used interchangeably with sensitive data.

A Data Steward is a senior-level employee of the Firm who oversees the lifecycle of one or more sets of Institutional Data. See the Information Security Roles and Responsibilities for more information.

Institutional Data is defined as all data owned or licensed by the Firm.

Non-public Information is defined as any information that is classified as Private or Restricted Information according to the data classification scheme defined in this Guideline.

Sensitive Data is a generalized term that typically represents data classified as Restricted, according to the data classification scheme defined in this Guideline. This term is often used interchangeably with confidential data.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Senior IT Executive
	HODs

SPECIFIC PROCEDURE

LCB Finance shall have data management guidelines for all applications or systems processes that involve data input/output and processing.

Data Entry Verification and Authorization

Data management guidelines shall define procedures that shall be followed to verify accuracy and completeness of data before entering the data into the LCB Finance's applications. Procedures shall also be in place to ensure that necessary approval or authorization (if required) is taken before entering the data into LCB Finance applications for processing if required.

LCB Finance's applications or systems shall handle incorrect inputs appropriately. Separation of duties shall be implemented for authorization and data entry functions to ensure integrity and accuracy of data. Output of applications and system processes shall be controlled so that only authorized personnel can access them. Outputs shall be periodically reviewed for accuracy and completeness by appropriate personnel.

Associated Procedures

The business process owners should inform the IT Department of the exact data entry requirements to be configured within data entry screens Additionally, the business process owners should develop any forms needed to guard and control data entry activities Once forms are finalized, copies of forms should be sent to the IT Department to verify that the data entry screen configurations are consistentto data entry format requirement. Access to data entry screens and/or paper forms should be authorized by the business process owners on a "need-to-have" and 'need-to- know" basis. Access authorizations requests should be sent to the IT Department.

Data Classification

To ensure that integrity and confidentiality of information is maintained, a data classification scheme shall be designed for LCB Finance. The level of security to be afforded to the data/information of LCB directly on the classification level of the data.

Information shall be disclosed only to those people who have a legitimate business requirement for the information. The data classification scheme shall be designed to support the "need to know", so that information is protected from unauthorized disclosure, use, modification, and deletion. Information shall be consistently protected throughout its life cycle, from its origination to its destruction.

Information shall be protected in a manner commensurate with its sensitivity; no matter where it resides, what form it takes, what technology was used to handle it, and what purpose it serves.

Associated Procedures

Although this data classification scheme provides overall guidance, to achieve consistent information protection, employees should apply and extend these concepts to address the requirements of day-to-day operations. A classification scheme should be structured as:

- Restricted
- Private / Confidential Internal
- Public

Based on the above classification, information asset owners should do proper labeling of information based on its sensitivity that should match the classification category of such information. Additionally, information asset owners should review their classification assignments regularly and should inform the IT Department of any changes no later than one week from date of change.

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the Entity should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels, or classifications:

A. Restricted
Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the Entity or its affiliates. Examples of Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data.

B. Private / Confidential - Internal
Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the Entity or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.

C. Public
Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the Entity and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Classification of data should be performed by an appropriate Data Steward in the IT Department. Data Stewards are senior-level employees of the Entity who oversee the lifecycle of one or more sets of Institutional Data in this instance the HOIT.

23.1.1. Data Collection

Data Stewards may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a Client's name, address and audited accounts, the data collection should be classified as Restricted even though the client's name and address may be considered Public information.

23.1.2. Reclassification

On a periodic basis, it is important to reevaluate the classification of Institutional Data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to the Entity. This evaluation should be conducted by the appropriate Data Steward. Conducting an evaluation on an annual basis; however, the Data Steward should determine what frequency is most appropriate based on available resources. If a Data Steward determines that the classification of a certain data set has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

23.1.3. Calculating Classification

Data classification reflects the level of impact to the Entity if confidentiality, integrity or availability is compromised.

	POTENTIAL IMPACT		
SECURITY OBJECTIVE	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

As the total potential impact to the Entity increases from Low to High, the classification of data should become more restrictive moving from Public to Restricted. If an appropriate classification is still unclear after considering these points, contact the Information Security Office for assistance.

Responsibility of IT Assets

- The IT Department shall clearly identify all Information assets.
- The IT Department shall draw up and periodically update an inventory of all Information assets.
- The IT Department in coordination with Business Departments shall assign an "Owner" (a person or a part of LCB Finance) to each asset associated with information processing facilities.
- The IT Department in coordination with Business Departments shall identify, document and implement rules for the acceptable use of asset associated with information processing facilities.

Associated Procedures

The IT Department should conduct an annual inventory of all information processing assets at LCB Finance. Once a complete list of information assets is finalized, the IT Department should assign all the information assets to Owners and an Asset Owner register should be developed and documented From there onwards, the IT Department is responsible for quarterly and requirement based updating of the Asset-Owner register and should integrate the change management process to identify and

reflect any changes in asset ownership assignments. An inventory of all relevant assets, including IT assets but not limited to, as well as the respective assigned owners will be in place (Configuration Management Database). An asset is an information, a storage medium or a system processing the information.

IT Assets and Information Classification

- LCB shall define classification criteria for all information assets.

Associated Procedures

The IT Department should establish the classification of IT assets criteria in terms of the assets: Value Legal requirements Sensitivity and criticality to LCB. Once the criteria information is obtained for each IT assets, the IT Department should classify all IT assets in LCB under the defined classification criteria.

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy
- Change Management Procedures
- Asset Management Procedures

External References

- CBSL Baseline Security Standards

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT or CEO, depending on the criticality. The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months). No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

24. SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE MANAGEMENT

PURPOSE

This policy is intended to establish the requirements for any System Acquisition, Development and Maintenance Management as a means of protecting the confidentiality, integrity and availability of the LCB Finance's information assets. It also sets out any relevant standards which those controls must meet.

INTRODUCTION

This document provides the LCB Finance's with the information required to effectively and efficiently plan, prepare and deploy solutions at LCB Finance. When properly implemented, this type of management provides an enhanced level of assurance that the system and data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception.

SCOPE

This section applies to any information system of LCB Finance in any format (paper or electronic), anyone who is involved its creation, maintenance and ultimate disposal. For any third party involved in this process, such security requirements are included in contracts and service level agreements. But the primary focus of the document is to provide guidance in the selection, acquisition and maintenance of systems for LCB Finance information. It applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance regardless of the geographic location.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	IT Executive

SPECIFIC PROCEDURE

Security Requirements

Business requirements for new systems or enhancements/amendments to the existing systems shall contain requirements for security controls. Risk assessments will identify security vulnerabilities and appropriate requirements are included in the requirement documentation.

Correct processing in applications

Appropriate controls and audit trails are built into the system. Input data is validated. Checks to include:

- Out of range values
- Invalid characters
- Missing or incomplete data

- Unauthorised or inconsistent use of data

Procedures exist to respond to such error reports when generated by the systems.

Output data of systems are validated by
- Reconciling control balances to verify that the data is processed accurately
- Verifying the plausibility of output using business rules specified
- Maintaining audit trails
- Providing error and exception reports

Security of system files

Implementation of the operational software shall be controlled.
- Updates are planned, approved, tested and have a roll-back plan.
- Users are notified of the changes and given additional training if necessary.
- New releases are assessed to see whether it will introduce security vulnerabilities
- It is ensured that developer ID is not present in production environment

Test data shall be protected.
- Sensitive or personal data is masked in test data
- Using production data as test data is properly authorized
- Output from test runs are marked as “Test”

Security in development and support process

Change control procedures

During system development or Customization
- Changes should be intimated by authorized persons
- Proposed changes are analyzed for impact as to time, cost etc
- All change requests are logged.

Changes for operational system
- Changes must be initiated by authorized persons
- All requests are logged in the CR tracking system
- Documenting and getting approval before making the changes in the system
- Document the acceptance test and obtain approval for the same
- Updating the security plan if the existing security is impacted by the proposed change
- Maintaining the version control of the software after the change

Changes to the operating system
- Sufficient time is taken to review the changes required
- The information security should not be compromised by the change
- The information system is tested fully in a test environment
- Business continuity plan shall be updated if required.

Information leakage should be prevented.
- Scan the system for malicious code
- Monitor resource usage in production systems
- Control third party network connections
- Regular monitoring

Control outsourced information system development.
- Procurement policy for doing such activity is followed.
- Escrow arrangements should be in place

- Rights of access for audit is built into the contract
- Quality and security requirements are written in the outsourcing contract

Vulnerability Management

Regular assessments shall be done to evaluate information system vulnerabilities and managing associated risks.

- Monitor external source of information on published vulnerabilities
- Assess the risk of such published vulnerabilities
- Evaluate options to minimize the impact of vulnerabilities
- Apply corrective measures to address the vulnerabilities

FORMS/TEMPLATES TO BE USED/REFERED

Not applicable

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy

External References

- ISO / IEC 27001-(1/2)

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department. Policy violations,standards and procedures of LCB Finance will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department.

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT and/or Director Finance depending on the criticality. The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months). At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

25. SECURITY CONFIGURATION POLICY

PURPOSE

Appropriate measures must be taken when configuring and managing server-based resources to ensure the confidentiality, integrity and availability of information. This policy provides general procedures and requirements for installing server-based resources in a secure manner as well as maintaining the security integrity of the hardware and application software. This hardening standard, in part, is taken from the guidance of the Center for Internet Security and NIST 800 – 123 is the result of a consensus baseline of security guidance from several government and commercial bodies. Other recommendations were taken from the Windows Security Guide, and the Threats and Counter Measures Guide developed by Microsoft.

INTRODUCTION

Hardware such as servers are in their many forms (file, print, application, web, and database) are used by the organization to supply critical information for staff. These assets must be protected from both security and performance related risks. One of the required steps to attain this goal is to ensure that hardware (whether on premise or in the cloud) is installed and maintained in a manner that prevents unauthorized access, unauthorized use, consistent configuration, and minimal service disruptions.

SCOPE

This policy applies to all LCB staff that use, deploy, or support LCB server hardware/virtual resources. All personnel are required to read, understand and comply with the IT and Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she shall consult with Head of IT or IT Department, business or functional manager as applicable for clarifications.

The IT Department shall assist resolve any conflicts arising from this Policy.

POLICY

A. General

A server hardening procedure shall be created and maintained that provides detailed information required to configure and harden LCB servers whether on premise or in the cloud. The procedure shall include:

- Installing the operating system from an IT approved source
- Applying all appropriate vendor supplied security patches and firmware updates
- Removing unnecessary software, system services, protocols, ports, and drivers
- Setting security and operational parameters including configuring system services, firewall, anti-virus, anti-malware, and local system passwords/accounts
- Enabling appropriate local file system/sharing permissions, audit logging, local/physical security, reporting, and intrusion detection software as applicable
- Applying LCB Domain-based Active Directory server-based group policy

B. Operations and Maintenance

LCB server support shall perform the following procedures and processes to ensure hardening compliance after the initial system is delivered:

- Post-Install operating system, utility/system service patches, database, web, and application security patches shall be pre-tested and deployed on a regular basis against similar systems before rolling out to the production environment.
- In the case of custom applications or enterprise software, LCB server support shall take appropriate precautions to ensure patch compatibility prior to install. Should a patch be incompatible with a specialized software package, exceptions must be approved in writing by the [Insert Appropriate Role] or their designee.
- All sensitive information shall be encrypted at-rest and in-transit as well as complying with the LCB Data Encryption Policy. Where appropriate, PKI certificates/key strategies shall be used to additionally secure web based access.
- Periodic audits of server compliance shall be conducted at least annually. Results shall be documented and any deficiencies corrected.

C. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the LCB internal processes and procedures. Examples of appropriate controls and documentation are:

- Documented server build processes and images
- Internal configuration and asset management protocols and procedures
- Patch logs containing server name, patch installed, service installed and date
- Documentation showing hardening and security measures employed across the enterprise
- Archival audit documentation with results and remedies taken to address security concerns

D. Associated Controls and Baseline Security Settings

Baseline Security Settings

Account Policies

1.1	Account Policies	Setting
1.1.1	Enforce password	24 remembered; not required to set for local accounts
1.1.2	Maximum password age	90 days (maximum)

1.1.3	Minimum password age	1 day or more
1.1.4	Minimum password length	8 characters
1.1.5	Password must meet complexity requirements	Enabled
1.1.6	Store passwords using reversible encryption	Disabled
1.1.7	Account lockout duration	15 minutes (minimum)
1.1.8	Account lockout threshold	10 attempts
1.1.9	Reset account lockout counter after	15 minutes (minimum)
1.1.10	Enforce user logon restrictions	Enabled
1.1.11	Maximum tolerance for computer clock synchronization	5
1.1.12	Maximum lifetime for service ticket	600
1.1.13	Maximum lifetime for user ticket renewal	7 days
1.1.14	Maximum lifetime for user ticket	10

Audit Policies

Windows Server 2008 has detailed audit facilities that allow administrators to tune their audit policy with greater specificity. By enabling the legacy audit facilities outlined in this section, it is probable that the performance of the system may be reduced and that the security event log will realize high event volumes. Given this, it is recommended that Detailed Audit Policies in the subsequent section be leveraged in favor over the policies represented below. Additionally, the "Force audit policy subcategory settings", which is recommended to be enabled, causes Windows to favor the audit subcategories over the legacy audit policies. For the above reasons, this Benchmark does not prescribe specific values for legacy audit policies.

1.2	**Audit Policy**	**Setting**

1.2.1	Audit Account Logon Events	Success and Failure
1.2.2	Audit Account Management	Success and Failure
1.2.3	Audit Directory Service Access	No Auditing
1.2.4	Audit Logon Events	Success and Failure
1.2.5	Audit Object Access	Failure (minimum)
1.2.6	Audit Policy Change	Success (minimum)
1.2.7	Audit Privilege Use	Failure (minimum)
1.2.8	Audit Process Tracking	No Audit
1.2.9	Audit System Events	Success (minimum)
1.2.10	Audit: Shut down system immediately if unable to log security audits	Disabled
1.2.11	Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled

Detailed Security Auditing

This section articulates the detailed audit policies introduced in Windows Vista and later. Prior to Windows Server 2008 R2, these settings could only be established via the auditpol.exe utility. However, in Server 2008 R2, GPOs exist for managing these items. Guidance is provided for establishing the recommended state using via GPO and auditpol.exe. The values prescribed in thissection represent the minimum recommended level of auditing.

1.3	**Detailed Security Auditing**	**Setting**
1.3.1	Audit Policy: System: IPsec Driver	Success and Failure

1.3.2	Audit Policy: System: Security State Change	Success and Failure
1.3.3	Audit Policy: System: Security System Extension	Success and Failure
1.3.4	Audit Policy: System: System Integrity	Success and Failure
1.3.5	Audit Policy: Logon-Logoff: Logoff	Success
1.3.6	Audit Policy: Logon-Logoff: Logon	Success and Failure
1.3.7	Audit Policy: Logon-Logoff: Special Logon	Success
1.3.8	Audit Policy: Object Access: File System	Failure
1.3.9	Audit Policy: Object Access: Registry	Failure
1.3.10	Audit Policy: Privilege Use: Sensitive Privilege Use	No auditing
1.3.11	Audit Policy: Detailed Tracking: Process Creation	Success
1.3.12	Audit Policy: Policy Change: Audit Policy Change	Success and Failure

1.3	**Detailed Security Auditing**	**Setting**
1.3.13	Audit Policy: Policy Change: Authentication Policy Change	Success
1.3.14	Audit Policy: Account Management: Computer Account Management	Success and Failure
1.3.15	Audit Policy: Account Management: Other Account Management Events	Success and Failure
1.3.16	Audit Policy: Account Management: Security Group Management	Success and Failure

1.3.17	Audit Policy: Account Management: User Account Management	Success and Failure
1.3.18	Audit Policy: DS Access: Directory Service Access	No Auditing
1.3.19	Audit Policy: DS Access: Directory Service Changes	No Auditing
1.3.20	Audit Policy: Account Logon: Credential Validation	Success and Failure

Event Log

1.4	**Event Log**	**Setting**
1.4.1	Application: Maximum Log Size (KB)	32768 KB or greater
1.4.2	Application: Retain old events	Disabled
1.4.3	Security: Maximum Log Size (KB)	81920 KB or greater
1.4.4	Security: Retain old events	Disabled
1.4.5	System: Maximum Log Size (KB)	32768 KB or greater
1.4.6	System: Retain old events	Disabled

Windows Firewall

1.5	**Windows Firewall**	**Setting**
1.5.1	Windows Firewall: Allow ICMP exceptions (Domain)	Disabled
1.5.2	Windows Firewall: Allow ICMP exceptions (Standard)	Disabled

1.5.3	Windows Firewall: Apply local connection security rules (Domain)	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is No.
1.5.4	Windows Firewall: Apply local connection security rules (Private)	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is No.
1.5.5	Windows Firewall: Apply local connection security rules (Public)	No
1.5.6	Windows Firewall: Apply local firewall rules (Domain)	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is No.
1.5.7	Windows Firewall: Apply local firewall rules (Private)	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is No.
1.5.8	Windows Firewall: Apply local firewall rules (Public)	No
1.5.9	Windows Firewall: Display a notification (Domain)	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.

		For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Yes.
1.5.10	Windows Firewall: Display a notification (Private)	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Yes.
1.5.11	Windows Firewall: Display a notification (Public)	No
1.5.12	Windows Firewall: Firewall state (Domain)	On
1.5.13	Windows Firewall: Firewall state (Private)	On
1.5.14	Windows Firewall: Firewall state (Public)	On
1.5.15	Windows Firewall: Inbound connections (Domain)	Block
1.5.16	Windows Firewall: Inbound connections (Private)	Block
1.5.17	Windows Firewall: Inbound connections (Public)	Block
1.5.18	Windows Firewall: Prohibit notifications (Domain)	Disabled
1.5.19	Windows Firewall: Prohibit notifications (Standard)	Disabled
1.5.20	Windows Firewall: Protect all network connections (Domain)	Enabled
1.5.21	Windows Firewall: Protect all network connections (Standard)	Enabled

Windows Update

1.6	Windows Update	Setting
1.6.1	Configure Automatic Updates	Enabled: 3 - Auto download and notify for install
1.6.2	Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Disabled
1.6.3	Reschedule Automatic Updates scheduled installations	Enabled

User Rights

1.8	User Rights	Setting
1.8.1	Access this computer from the network	For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is Administrators, Authenticated Users. For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS.
1.8.2	Act as part of the operating system	No one
1.8.3	Adjust memory quotas for a process	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators, LOCAL SERVICE, NETWORK SERVICE. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.4	Back up files and directories	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators.

		For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.5	Bypass traverse checking	For the Enterprise Member Server profile(s), the recommended value is Administrators, Authenticated Users, Backup Operators, Local Service, Network Service. For the Enterprise Domain Controller profile(s), the recommended value is Not Defined. For the SSLF Domain Controller profile(s), the recommended value is Authenticated Users, Local Service, Network Service. For the SSLF Member Server profile(s), the recommended value is Administrators, Authenticated Users, Local Service, Network Service.
1.8.6	Change the system time	LOCAL SERVICE, Administrators
1.8.7	Create a pagefile	For the Enterprise Member Server, SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.8	Create a token object	No One
1.8.9	Create global objects	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators,

		SERVICE, Local Service, Network Service.
1.8.10	Create permanent shared objects	No One
1.8.11	Debug programs	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Administrators. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is No one.
1.8.12	Deny access to this computer from the network	Guests
1.8.13	Enable computer and user accounts to be trusted for delegation	No One
1.8.14	Force shutdown from a remote system	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.15	Impersonate a client after	For all profiles, the recommended state for this setting is Administrators, SERVICE, Local Service, Network Service.
1.8.16	Increase scheduling priority	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.

1.8.17	Load and unload device drivers	Administrators
1.8.18	Lock pages in memory	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is No one. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.19	Manage auditing and security log	For the Enterprise Member Server, SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.20	Modify firmware environment values	For the Enterprise Member Server, SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.21	Perform volume maintenance tasks	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.22	Profile single process	Administrators
1.8.23	Profile system performance	Administrators
1.8.24	Remove computer from docking station	Administrators

1.8.25	Replace a process level token	For all profiles, the recommended state for this setting is LOCAL SERVICE, NETWORK SERVICE.
1.8.26	Shut down the system	Administrators
1.8.27	Add workstations to domain	For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is Not Defined.
1.8.28	Allow log on locally	Administrators
1.8.29	Allow log on through Terminal Services	Do not disable; Limit via FW - Access via UConn networks only
1.8.30	Change the time zone	For all profiles, the recommended state for this setting is LOCAL SERVICE, Administrators.
1.8.31	Create symbolic links	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.32	Deny log on locally	Guests
1.8.33	Deny log on through Terminal Services	Guests
1.8.34	Generate security audits	For the Enterprise Member Server, SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is LOCAL SERVICE,

		NETWORK SERVICE.For the Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.35	Increase a process working set	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators, Local Service for the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.8.36	Log on as a batch job	For the Enterprise Domain Controller,SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is No one.For the Enterprise Member Server profile(s), the recommended value is Not Defined.
1.8.37	Restore files and directories	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Administrators.For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Administrators, Backup Operators.
1.8.38	Take ownership of files or other objects	Administrators
1.8.39	Access credential Manager as a trusted caller	No One
1.8.40	Synchronize directory service data	No One

Security Options

1.9	**Security Options**	**Setting**

1.9.1	Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	For all profiles, the recommended state for this setting is Require NTLMv2 session security, Require 128-bit encryption.
1.9.2	Network access: Remotely accessible registry paths and sub-paths	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is: System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog Other Domain Controller profile(s), are Not Defined.
1.9.3	Accounts: Rename administrator account	For all profiles, the recommended state for this setting is any value that does not contain the term "admin".
1.9.4	Accounts: Rename guest account	For all profiles, the recommended state for this setting is any value that does not contain the term "guest".
1.9.5	Accounts: Guest account status	Disabled
1.9.6	Network access: Allow anonymous SID/Name translation	Disabled
1.9.7	Accounts: Limit local account use of blank passwords to console logon only	Enabled
1.9.8	Devices: Allowed to format and eject removable media	Administrators

1.9.9	Devices: Prevent users from installing printer drivers	Enabled
1.9.10	Devices: Restrict CD-ROM access to locally logged-on user only	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.9.11	Devices: Restrict floppy access to locally logged-on user only	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled.For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.9.12	Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
1.9.13	Domain member: Digitally encrypt secure channel data (when possible)	Enabled
1.9.14	Domain member: Digitally sign secure channel data (when possible)	Enabled
1.9.15	Domain member: Disable machine account password changes	Disabled
1.9.16	Domain member: Maximum machine account password age	For all profiles, the recommended state for this setting is 30 day(s).
1.9.17	Domain member: Require strong (Windows 2000 or later) session key	Enabled
1.9.18	Domain controller: Allow server operators to schedule tasks	For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is Disabled. For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is Not Defined.
1.9.19	Domain controller: LDAP server signing requirements	For the SSLF Domain Controller profile(s), the recommended value is Require signing. For the Enterprise Member Server, Enterprise

		Domain Controller and SSLF Member Server profile(s), the recommended value is Not Defined.
1.9.20	Domain controller: Refuse machine account password changes	For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is Disabled. For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is Not Defined.
1.9.21	Interactive logon: Do not display last user name	Enabled
1.9.22	Interactive logon: Do not require CTRL+ALT+DEL	Disabled
1.9.23	Interactive logon: Number of previous logons to cache (in case domain controller is not available)	For all profiles, the recommended state for this setting is 1 logon.
1.9.24	Interactive logon: Prompt user to change password before expiration	14 days (see netid.uconn.edu)
1.9.25	Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled
1.9.26	Interactive logon: Smart card removal behavior	Lock Workstation
1.9.27	Omitted	
1.9.28	Omitted	
1.9.29	Interactive logon: Require smart card	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.

1.9.30	Microsoft network client: Digitally sign communications (always)	Enabled
1.9.31	Microsoft network client: Digitally sign communications (if server agrees)	Enabled
1.9.32	Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
1.9.33	Microsoft network server: Amount of idle time required before suspending session	15 minutes
1.9.34	Microsoft network server: Digitally sign communications (always)	Enabled
1.9.35	Microsoft network server: Digitally sign communications (if client agrees)	Enabled
1.9.36	Microsoft network server: Disconnect clients when logon hours expire	Disabled
1.9.37	Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
1.9.38	Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
1.9.39	Network access: Do not allow storage of credentials or .NET Passports for network authentication	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.9.40	Network access: Let Everyone permissions apply to anonymous users	Disabled

1.9.41	Network access: Named Pipes that can be accessed anonymously	For the SSLF Member Server profile(s), the recommended value is browser. For the SSLF Domain Controller profile(s), the recommended value is: netlogon, lsarpc, samr, browser. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.9.42	Network access: Remotely accessible registry paths	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion
1.9.43	Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
1.9.44	Network access: Shares that can be accessed anonymously	None
1.9.45	Network access: Sharing and security model for local accounts	For all profiles, the recommended state for this setting is Classic - local users authenticate as themselves.
1.9.46	Network security: Do not store LAN Manager hash value on next password change	Enabled
1.9.47	Network security: LAN Manager authentication level	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Send NTLMv2 response only. Refuse LM. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Send NTLMv2 response only. Refuse LM & NTLM.
1.9.48	Network security: LDAP client signing requirements	Negotiate signing
1.9.49	Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security, Require 128-bit encryption

1.9.50	Recovery console: Allow automatic administrative logon	Disabled
1.9.51	Recovery console: Allow floppy copy and access to all drives and all folders	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Disabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.9.52	Shutdown: Clear virtual memory pagefile	Disabled
1.9.53	Shutdown: Allow system to be shut down without having to log on	Disabled
1.9.54	System objects: Require case insensitivity for non-Windows subsystems	Enabled
1.9.55	System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
1.9.56	System cryptography: Force strong key protection for user keys stored on the computer	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is User must enter a password each time they use a key. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is User is prompted when the key is first used.
1.9.57	System settings: Optional subsystems	None
1.9.58	System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.9.59	MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Disabled

1.9.60	MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	For all profiles, the recommended state for this setting is Highest protection, source routing is completely disabled.
1.9.61	MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Disabled
1.9.62	MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is 5 minutes. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.9.62	MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is 5 minutes. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.9.63	MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic	For all profiles, the recommended state for this setting is Only ISAKMP is exempt (recommended for Windows Server 2003).
1.9.64	MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Enabled
1.9.65	MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)	Enabled
1.9.66	MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	Disabled
1.9.67	MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	Enabled

1.9.68	MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	0
1.9.69	MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	3
1.9.70	MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	90% or less
1.9.71	MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)	For all profiles, the recommended state for this setting is Highest protection, source routing is completely disabled.
1.9.72	MSS: (TCPMaxDataRetransmissions) IPv6 How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	3

Terminal Services

1.10	**Terminal Services**	**Setting**
1.10.1	Always prompt client for password upon connection	Enabled
1.10.2	Set client connection encryption level	Enabled: High Level
1.10.3	Do not allow drive redirection	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled.

1.10.4	Do not allow passwords to be saved	Enabled

Internet Communications

1.11	Internet Communication	Setting
1.11.1	Turn off downloading of print drivers over HTTP	Enabled
1.11.2	Turn off the "Publish to Web" task for files and folders	Enabled
1.11.3	Turn off Internet download for Web publishing and online ordering wizards	Enabled
1.11.4	Turn off printing over HTTP	Enabled
1.11.5	Turn off Search Companion content file updates	Enabled
1.11.6	Turn off the Windows Messenger Customer Experience Improvement Program	Enabled
1.11.7	Turn off Windows Update device driver searching	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.

Additional Security Settings

1.12	Additional Security Settings	Setting
1.12.1	Do not process the legacy run list	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the SSLF Member Server and SSLF Domain Controller

		profile(s), the recommended value is Enabled.
1.12.2	Do not process the run once list	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled.
1.12.3	Registry policy processing	For the Enterprise Member Server and SSLF Member Server profile(s), the recommended value is Enabled (Process even if the Group Policy objects have not changed). For the Enterprise Domain Controller and SSLF Domain Controller profile(s), the recommended value is Not Defined.
1.12.4	Offer Remote Assistance	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Disabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.12.5	Solicited Remote Assistance	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Disabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.12.6	Restrictions for Unauthenticated RPC clients	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled: Authenticated. For the Enterprise Member

		Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.12.7	RPC Endpoint Mapper Client Authentication	For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Enabled. For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Defined.
1.12.8	Turn off Autoplay	Enabled: All drives
1.12.9	Enumerate administrator accounts on elevation	For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is Not Configured. For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is Disabled.
1.12.10	Require trusted path for credential entry	Enabled
1.12.11	Disable remote Desktop Sharing	Enabled

INTERNAL AND EXTERNAL REFERENCES

Internal References

- IT Security Policy
- IT Security and Risk Management Policy
- IT Asset Management Policy
- Network Management Policy

External References

- NIST Framework

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department and the Risk department.

Violations of the policies, standards and procedures of LCB Sri Lanka will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment
- Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department

EXCEPTIONS

This policy is intended to address Operating Systems Security requirements. Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT /or Manager - IT, depending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months). At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

The waiver shall be monitored to ensure its concurrence with the specified period for any exceptions.

All exceptions to this policy must be communicated through the Policy Waiver Request Form.

26. CLEAR DESK AND SCREEN POLICY

PURPOSE

This policy is intended to establish the requirements in terms protecting the confidentiality, integrity and availability of the LCB Finance's information assets. The Clear Desk, Clear Screen Policy will help ensure that all sensitive/confidential materials are removed from workspaces and locked away when the items are not in use or an employee leaves their workstation. The policy will help reduce the risk of security breaches within the workplace. It also sets out any relevant standards which those controls must meet.

INTRODUCTION

This document provides the LCB Finance's with the information required to effectively and efficiently secure information assets at LCB Finance. When properly implemented, this type of management provides an enhanced level of assurance that the data cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception.

SCOPE

This section applies to any information asset of LCB Finance in any format (paper or electronic), anyone who is involved its creation, maintenance and ultimate disposal. It applies to all users of information assets including permanent or temporary employees, employees of temporary employment agencies, vendors, business partners, and/or contractor personnel and functional units in LCB Finance regardless of the geographic location.

RESPONSIBILITIES

The sponsor of this policy & procedure is the Head of IT, LCB Finance. The IT Department is responsible for the accuracy, completeness, accuracy, validity and reliability of the document. Any enquiries regarding this policy shall be directed to the IT Department.

Role	Designation
Process Owner	Head of IT
Process delegates	Head of Departments, Assistant Manager – IT IT Executive

SPECIFIC PROCEDURE

CLEAR DESK POLICY

i. Where practically possible, paper and computer media should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.

ii. Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office doors must be locked if left unattended.

iii. Hard copy documents containing any personal data, or confidential, restricted or sensitive information should only be stored if necessary. e.g original legal papers which must be served. Where appropriate, documents should always be scanned to PDF and stored within the dedicated case file on LCB Finance's secure servers.

iv. Original paper copies should be securely stored in confidential shredding bags for destruction.
v. Employees are required to ensure that all confidential, restricted or sensitive information in hardcopy or electronic form is secured at the end of the day and when they are expected to be away from their desk for an extended period.
vi. Any confidential, restricted or sensitive information must be removed from desks and locked in a drawer when a desk is left unoccupied at any time.
vii. Confidential, restricted or sensitive information, when printed, should be cleared from printers immediately. Where possible printers with a 'locked job' facility should be used.
viii. It is good practice to lock office areas when they are not in use and it is safe to do so.
ix. Any visit, appointment or message books should be stored in a locked area when not in use.
x. The reception area can be particularly vulnerable to visitors. This area should be kept as clear as possible at all times. No personally identifiable information should be kept on desks within reach or sight of visitors.
xi. It is also worth noting that information left on desks is also more likely to be damaged or destroyed in a disaster such as fire, flood or explosion.
xii. Keys used for access to confidential, restricted or sensitive information must not be left in or on an unattended desk. Keys for desk drawers, cabinets and other secure areas must be stored in the dedicated key safe.
xiii. Upon disposal, any document containing any personal data or confidential, restricted or sensitive information should be placed in the confidential shredding bags which are stored in locked secure locations. Confidential waste must not be left on desks, in filing trays or placed in regular waste bins.

Clear Screen Policy

i. Computer terminals should not be left logged on when unattended and should always be password protected.
ii. Computer screens should be angled away from the view of unauthorized persons.
iii. Computer workstations must be logged off at the end of the working day, to allow security updates to be installed during the evening.
iv. The Windows Security Lock should be set to activate when there is no activity for a short pre-determined period of time.
v. The Windows Security Lock should be password protected for reactivation.
Passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down and left in an accessible location.
vi. Users should log off or lock their machines (by pressing the Windows key and L) when they leave the room.
vii. Whiteboards containing restricted and/or sensitive information should be erased.
viii. Portable computing devices such as unused laptops, digital cameras and tablets must be locked away in a drawer or the server room.

ix. Mass storage devices such as CDROM, DVD or USB drives should be treated as being sensitive data and must locked away in a drawer or the server room.

Maintaining Compliance

i. Regular and ongoing Clear Desk, Clear Screen audits will be undertaken to ensure continued employee compliance with this policy.
ii. Clear Desk, Clear Screen audits will be documented and logged as per LCB Finance's documented 'Clear Desk Audit Process'. This process will be reviewed annually. It is the responsibility of the Head of IT to ensure reviews take place.
The auditee must provide the relevant employees name, date of the audit and tick Pass or Weakness for each section. Any identified issues or areas of weakness should also be documented.
iii. Where a weakness has been logged, the auditee must email that member of staff with the following example text.
iv. Both the above email and the signed scanned audit report should then be logged in the relevant employees file under the disciplinary section and reported to the employee's line manager.
v. Further training will be provided when and where required.
vi. Persistent and repeated breaches of the policy should be referred to the Manager - Information Security.

FORMS/TEMPLATES TO BE USED/REFERED

Not applicable

INTERNAL AND EXTERNAL REFERENCES

Internal References

- Information Security Policy

External References

- ISO / IEC 27001-(1/2)

COMPLIANCE

Compliance with this Procedure is mandatory. The Head of IT must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department.

Violations of the policies, standards and procedures of LCB Finance will result in corrective/preventive actions by management.

Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Termination of Employment

Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department.

EXCEPTIONS

Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the Head of IT and/or CEO dedepending on the criticality.

The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months). At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary.

No policy/procedure shall be provided waiver for more than three consecutive terms. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

[THIS PAGE IS INTENTIONALLY LEFT BLANK]