

# Global IME Bank

ग्लोबल आइएमई बैंक लि.

सबैका लागि बैंक


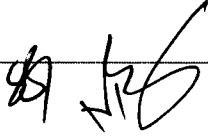


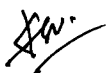
## Information Security Policy

Revised: August 2020

संचालक समितिको गित २०६६-०६-०४को  
२६९ को बैठकबाट स्वीकृत ।

## Preamble

In exercise to the power conferred by Section 22 of Bank and Financial Institution Act 2073 and the Article of Association of Global IME Bank Limited, the Board of Directors of Global IME Bank Ltd has approved this policy vide its \_\_\_ Board Meeting dated \_\_\_\_\_ for implementation. This policy has been prepared in accordance with Information Technology Guidelines 2012 and Nepal Rastra Bank( Central Bank) Directive/Circulars and amendments thereof issued time to time.

**Version Control**

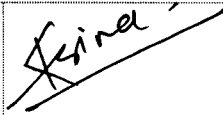
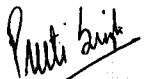
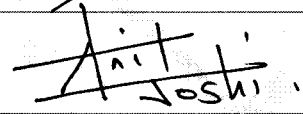
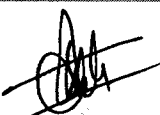

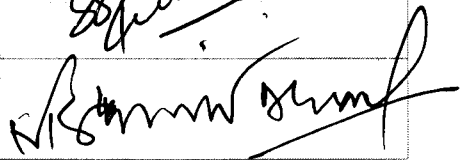
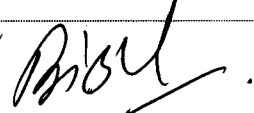
| Version Control No. | Date          | Remarks |
|---------------------|---------------|---------|
| Version 1           | April 2013    | Revised |
| Version 2           | November 2017 | Revised |
| Version 3           | August 2020   | Revised |



(i)



## Approval Sheet

|               |  |   |
|---------------|--|---|
| Prepared By : | Kimil Timilsina<br>ISO                                   |    |
|               |  |   |
| Reviewed By : | Preeti Singh<br>Manager- Strategy                        |    |
|               | Anil Joshi<br>Chief Information Technology Officer       |    |
|               | Buddhi Akela<br>Chief Risk Officer                       |    |
| Supported By: | Sujit Kumar Shakya<br>Dy. Chief Executive Officer        |   |
|               | Mahesh Sharma Dhakal<br>Acting Chief Executive Officer   |   |
| Approved By : | Board of Directors<br>BOD Meeting: 361 Date: 20-Sep-2020 |  |

## Table of Contents

**PREAMBLE**

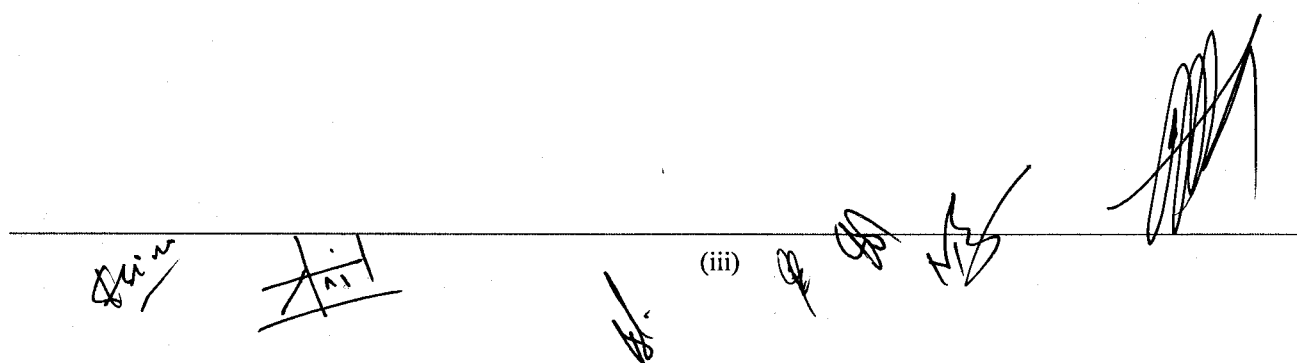
**VERSION CONTROL**

**APPROVAL SHEET**

**TABLE OF CONTENTS**

|                   |   |
|-------------------|---|
| <b>CHAPTER 1</b>  | <b>INTRODUCTION AND SCOPE</b>   |
| <b>CHAPTER 2</b>  | <b>RISK ASSESSMENT</b>  |
| <b>CHAPTER 3</b>  | <b>INFORMATION / INVENTORY ASSETS CLASSIFICATION AND CONTROL POLICY</b> |
| <b>CHAPTER 4</b>  | <b>PHYSICAL AND ENVIRONMENT CONTROLS</b>                                |
| <b>CHAPTER 5</b>  | <b>USER AUTHENTICATION</b>  |
| <b>CHAPTER 6</b>  | <b>PENETRATION TESTING AND SYSTEM UPDATES</b>                           |
| <b>CHAPTER 7</b>  | <b>SYSTEM CONFIGURATION AND HARDENING</b>                               |
| <b>CHAPTER 8</b>  | <b>ANTIVIRUS POLICY</b>   |
| <b>CHAPTER 9</b>  | <b>AUDIT TRAIL</b>  |
| <b>CHAPTER 10</b> | <b>DATA RETENTION AND DISPOSAL POLICY</b>                               |
| <b>CHAPTER 11</b> | <b>NETWORK INFRASTRUCTURE SECURITY</b>                                  |
| <b>CHAPTER 12</b> | <b>REMOTE ACCESS</b>  |
| <b>CHAPTER 13</b> | <b>BACKUP POLICY</b>  |
| <b>CHAPTER 14</b> | <b>INCIDENT RESPONSE PLAN AND PROCEDURES</b>                            |
| <b>CHAPTER 15</b> | <b>ENCRYPTION POLICY</b>  |
| <b>CHAPTER 16</b> | <b>USAGES POLICY FOR CRITICAL INFORMATION ASSETS/TECHNOLOGY</b>         |
| <b>CHAPTER 17</b> | <b>CHANGE MANAGEMENT POLICY</b>   |
| <b>CHAPTER 18</b> | <b>MISCELLANEOUS</b>  |

*This document contains 31 Pages excluding the cover page.*



## CHAPTER 1 Introduction and Scope

This document is a policy issued by Global IME Bank to ensure that all information technology users are within the domain of the organization or its network and comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization boundaries of authority. Global IME Bank management has committed to these security policies to protect information utilized by Global IME Bank in attaining its business goals. All employees are required adhere to the policies described within this document.

The need of Information Security Policy has been also addressed in Nepal Rastra Bank Information Technology Guidelines 2012. The guidelines require Information Security Policy to be approved by Board of Directors and Information Security Officer (ISO) shall be responsible for enforcing Information security policy of the Bank.

### 1.1 Policy Roles and Responsibility

Information Security Policies addresses all electronic delivery channels and payment system and requires it to be communicated to all employees, contractors/suppliers, consultants and officials.

All employees, contractors, vendors and third-parties that use, maintain or handle GIBL information assets must follow this policy.

### 1.2 Information Security Officer (ISO)

ISO is responsible for enforcing information security policy in Bank. ISO is also responsible for coordinating and communicating security related issues within the organization or with relevant external organization. ISO need to comply with Confidentiality, Integrity and Availability of its information assets.

The ISO works closely with other staffs in securing the GIBL information assets and enforcing established policies and guidelines. Responsibilities of ISO includes:

- Creates information security strategies, both short-term and long-range, in support of the GIBL goals.
- Communicates risks and recommendations to mitigate risks to the senior administration by communicating in non-technical, cost/benefit terms and in a format relevant to senior administrators so decisions can be made to ensure the security of information systems and information entrusted to the GIBL
- Make decision pertaining to the information securities policies and their content.
- Conduct Risk assessment periodically for each asset that has possibility of impacting the Information Security Principle -Confidentiality, Integrity and Availability.
- Annually review the Information Security Policy to cover the latest change in business requirement or security threats.
- Make sure access authorization for information of the Bank provided on need to know basis with least privilege.
- Make sure that all third parties, with whom confidential data is shared, are handled properly.
- Review system vulnerabilities and penetration testing and IT audits conducted and ensure findings are sufficiently addressed.

### 1.3 Information Security Unit (ISU)

ISU is responsible for implementing and maintaining organization-wide information security policies, standards, guidelines, and procedures. ISU shall provide security awareness education and ensure that everyone knows his or her role in maintaining security. ISU works with departmental system managers, administrators and users to develop securities policies, standards and procedures to help protect the assets of GIBL.

#### Responsibilities of Information Security Unit (ISU):

- Maintain and Review the existing Information Security Policy periodically for identifying latest threats and changes in modus operandi of electronic attacks.
- Act as a central coordinating department for implementation of the Information Security Policies.
- ISU review logs daily. Follow up on any exceptions identified and follow Incident Response Plan if applicable.
- Control and monitor access to restricted areas and confidential data.
- Complete tasks delegated by ISO
- Monitor the configuration of all GIBL applications to ensure they meet the standards set forth in the Information Security Program.
- Oversee the quarterly review of employee access rights to Bank systems to verify alignment with job responsibilities.
- Continue to enhance the Information/ Cyber Security Awareness Programs for employees and customers.
- Initialize the International Best Practice for proactive risk assessment and Employee Awareness and Capacity Development related to Cyber Security.

### 1.4 System /Network Administrators

GIBL System Administrators has the direct link between Information Security Policies and the network, systems, and data.

- Apply GIBL Information Security Policy and Procedure as applicable to all information systems.
- Assist Information Security Unit in monitoring access to GIBL data
- Network Administrator has to maintain up to date network diagram including wireless networks. The diagram must include the date when it was last updated.
- Restricting physical access to publicly accessible network jacks, wireless access points, gateways and hand held devices.

### 1.5 Human Resources Department

- Assist the Information Security Unit with publishing and disseminating GIBL information security policies and acceptable use guidance to all relevant system users, including vendors, contractors and business partners.
- Perform background checks on all employees.
- Work with the Information Security Unit to administer sanctions and disciplinary action relative to violations of Information Security Policy.
- Notify the Information Security Unit when any employee is recruited, transferred, or terminated.

## 1.6 End Users

Every user of GIBL resources should realize the fundamental importance of keeping their information asset safe. The responsibilities of all GIBL users are:

- It is the responsibility of users to safeguard their documents against the threat.
- Act according to Information Security Policy



## CHAPTER 2 Risk Assessment

Information Security Officer must coordinate an annual formal risk assessment process that identifies any existing or new threats and vulnerabilities to ensure GIBL assets are adequately protected. Risk assessments are used to identify, estimate and prioritize risks to organizational operations and assets resulting from the operation and use of information systems.

Risk assessment involves only three factors: the importance of the assets at risk, how critical the threat is, and how vulnerable the system is to that threat.

$\text{Risk} = \text{Asset} \times \text{Threat} \times \text{Vulnerability}$

The risk assessment should be based on mature methodology such as ISO/IEC 27005 or National Institute of Standards and Technology Special Publication Rev 1. 800-30" Guide for conducting Risk Assessments", or any other national/international framework developed.

## CHAPTER 3      **Information / Inventory Assets Classification and Control Policy**

Information Security Policy Addresses Information and Inventory assets in GIBL should be recorded and classified according to criticality of information. Security requirement and corresponding access control mechanism should be developed for each class and it should commensurate with level of criticality of information.

All data stored on GIBL information systems, whether managed by employees or by a third party, must follow this policy.

### 3.1 Data Classification

Information Asset Classification, in context of Information Security, is the classification of Information based on its level of sensitivity and the impact to the GIBL. The classification of information helps determine what baseline security controls are appropriate for safeguarding that information. All GIBL information should be classified into one of the three sensitivity tiers, or classifications.

- a. **Tier 1: Public Information:** Applies to all other information which does not clearly fit into any of the internal and restricted classifications. Unauthorized disclosure isn't expected to seriously or adversely impact the company. Any release of this information must be authorized by concerned Department. Examples of Public Information: GIBL website, Published Annual Reports, Published Marketing Information.
- b. **Tier 2: Internal Information:** Applies to sensitive business information which is intended for use within GIBL. Unauthorized disclosure could adversely impact the company, its stockholders, its business partners, and/or its customers. Examples of internal information include, internal market research, audit reports, policies and procedures, intellectual property etc.
- c. **Tier 3: Restricted Information:** Applies to the most sensitive business information which is intended strictly for use within GIBL. Unauthorized disclosure could seriously and adversely impact the company, stockholders, business partners, and/or its customers. Examples of restricted information include but are not limited to: credit card information, swift information, company private information, corporate strategies, competitor sensitive data, trade secrets, specifications, customer lists, and research data.

### 3.2 Data Access Policy

Access Authorization for information of the GIBL should be in "need to know" basis and with least privilege and should be for required time only. GIBL should closely supervise individuals with privilege access to the system. With their system activities logged, access to system by privilege users should be done by strong controls and security practices.

All Restricted data must be protected via access controls to ensure that data is not improperly disclosed, modified, deleted or rendered unavailable. Logs must track all access to such data and identify who and when the data was accessed.

Employees who have been authorized to view information at a particular classification level only be permitted to access information at that level or at a lower level on a need to know basis. All access to systems must be configured to deny all but what a particular user needs to access per their business role.

Access to systems or applications handling Restricted, Internal and Public Information must follow the data access request process.

Access to data must be based on role matrix approved by GIBL. Access to data exceeding the employee's authorized role must also follow the data access request process and must include documented limits around such access (e.g. access source, access time limits, etc.).

## CHAPTER 4 Physical and Environment Controls

GIBL must implement appropriate physical and environment controls taking into consideration of threats, and based on the entity's unique geographical location, building configuration, neighboring entities etc. to secure critical hardware, system and information.

Hardcopy material and electronic media devices containing restricted or internal information must be protected by physical and environment controls procedures:

- CCTV cameras and logged access control must be kept at entry and exit point for monitoring. CCTV cameras should record footage of minimum 3 months.
- CCTV at each ATM location must be installed with adequate lighting inside ATM center so as to capture clear picture of person doing ATM operations. CCTV must not capture the PIN entered by customer. Secure Transmission of Message using appropriate encryption from ATM, controls relating to ATM key generation, loading, destruction, firewall, antivirus, secure PIN generation, adequate segregation of duty while creating PIN and Card must be employed.
- GIBL should ensure that electronic card and its PIN is not under control of single person from the point of production till it is delivered to customer. PIN and card should not be together at any point of time before it reaches to customer hand. Internal Audit Department or Information Security Unit through any means identify the issues and communicate the risk to Information Security Officer.
- Restricted and Internal data access environment must be controlled through badge system or biometric device access. Information Security Unit must verify whether the internal and restricted data has been as per the Information Security Policy of the Bank.
- Visitor logs and access logs to sensitive data environment must be kept and reviewed quarterly by Information Security Unit and report to Information Security Officer.
- Publicly accessible network port must be enabled only when needed by authorized personnel and disabled after the use.

## CHAPTER 5 User Authentication

The policy is designed to protect GIBL equipment and the information contained within that equipment by providing guidelines on handling the password as well as setting requirements for strong password.

### 5.1 Password handling guidelines for individuals

All GIBL employee and external user shall follow the guidelines below to keep their password safe.

- Password shall never be written down.
- Password shall be never be sent over email if the said email is not encrypted.
- Password shall never be stored in a non-encrypted document.
- Password shall never be stored on mobile phones.
- Password shall not be shared via SMS or other unencrypted method via phone.
- Individual password shall not be shared with anyone else.
- Password shall never be revealed over telephone.
- Individual password format shall never be hinted at.
- Password shall never be revealed or hinted at on a form on the internet.
- The "Remember Password" feature of application programs such as Internet Explorer, Outlook, or any other program shall never be used for GIBL related user accounts.
- The password for GIBL accounts shall never be used on an account over the internet. If a password is suspected to be compromised, it shall be reported to IT support and changed immediately.
- Common acronyms shall not be used as part of the password.
- Common words or reverse spelling of words shall not be used as password.
- Names of people or places shall not be used as password.
- The login name shall not be a part of the password. Parts of numbers easily remembered such as phone numbers, date of birth shall not be a part of the password.

### 5.2 Password Requirement for System Owners

- Password shall be at least 8 characters long.
- Password shall contain alphanumeric:
- One special character such as !@#\$%^&\*
- Last 3 passwords history not to be repeated.
- Password shall be changed regularly. The period shall be based on documented risk assessment and agreed with Information Security Officer, else the following default shall be followed.
  - a. For user level password- (E.g. Domain Password)- 90 days
  - b. For application/ database level password (E.g. –Database/ Application)- 90 days
  - c. For system level password (E.g.: root and sys admin password)-90 days
- Passwords used for integration with different systems shall be changed frequently. The period shall be based on documented risk assessment and agreed with Information Security Officer, else a default of 90 days shall be used.
- Account lockout threshold shall be minimum 3 failed login attempts. If there are minimum 3 failed login attempts from the same account with minimum 15 minutes, the account shall be locked out.
- The account lockout shall be for minimum 15 minutes. The session shall be timed out and user shall be logged out within 5 minutes of user inactivity. User shall be required to put in passwords to log in again including to the laptop.

- Password shall not be same for public and private key authentication.
- Password shall be encrypted during transfer over networks.
- Passwords shall not be displayed on screen when entered.
- Password files shall be stored in one way encrypted form and separated from application files, in order to prevent exposure in case of a data intrusion.
- Password shall not be shared together with username and system information via SMS.
- If password needs to be shared over SMS, no other information identifying the system or username shall be shared.

### 5.3 User Account Requirement

System owners shall follow the requirements below for user accounts in their systems:

- User account shall be personal.
- User ID's shall be unique and personal. Group account shall not be allowed in any systems. Exceptions need to be documented and agreed with relevant information owner and Information Security Officer.
- All default system accounts shall be disabled. Any exception to the points above shall be agreed upon with the Information security officer and properly documented.

## CHAPTER 6 Penetration Testing and System Updates

### 6.1 Penetration Testing

Penetration testing involves the use of a variety of manual and automated techniques to simulate an attack on an organization's information security arrangements. It should be conducted by a qualified and independent penetration testing expert, sometimes referred to as an ethical security tester. Penetration testing looks to exploit known vulnerabilities but should also use the expertise of the tester to identify specific weaknesses – unknown vulnerabilities - in an organization's security arrangements. The penetration testing process involves an active analysis of the target system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, and Operational weaknesses in process or technical countermeasures. This analysis is typically carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

Information Security Unit is responsible for conducting penetration testing of the system and network internally and externally. Information Security Unit can itself conduct Penetration testing or outsource external professional provider for conducting penetration testing. The penetration testing should be conducted at least periodically for accessing the vulnerabilities in system and network.

### 6.2 Security Patch Deployment

All security patches, hot-fixes and service packs identified by the Information Security Unit or the System Administrator, must be installed on server/ application systems. Patch installation shall be applied based on a previous risk analysis. All installation of patches must follow the Change Management Policy.

## CHAPTER 7 System Configuration and Hardening

### 7.1 System Configuration Policy

All system, prior to deployment in the production environment must confirm to the System Configuration Standards. A valid justification and risk assessment must exist for all deviations.

System configuration record must be completed for all deployment systems at the time of installation and kept the document/ record as long as system is in service.

#### System Configuration Process:

- Install Operating System.
- Update Operating System software
- Configure Operating System as per System Configuration Standards.
- Install applications and software as per approved list.
- Update all application software
- Configure application parameters according to the System configuration standards for hardening.
- Enable Audit Trail
- Ensure that all vendor supplied defaults are changed before the system goes into production.
- Verify that insecure ports, services and demons, such as FTP, TELNET, POP3, IMAP, NetBIOS, and File Sharing are never used in the Production environment or are protected using technologies like SSH, SFTP, SSL, or IPsec VPN. If any insecure ports, services or demons are used, there must be a written justification and documentation of the security features used to compensate for the risk.



## CHAPTER 8 Antivirus Policy

All systems must be configured with Antivirus software. The anti-virus solution must be able to detect, remove and protect against all known types of malicious software such as viruses, Trojans, worms, spyware, adware, and rootkits. The software must be configured to receive automatic updates, perform periodic scans, log anti-virus events with routing to a central logging solution, and end users must not be able to configure or disable the software. All systems with anti-virus software must be configured to update virus signatures and scan engines on at least daily basis.

Retention of Anti-virus software logs will be in accordance with the Data Retention and Disposal Policy.

**CHAPTER 9      Audit Trail**

Automated Audit trails must be implemented for all system components. Audit trail must be available for each application handling sensitive information of the Bank. Audit trail shall be details enough to comply with regulatory, legal and Bank's requirement and should be secured to ensure integrity of the information. Audit trail must be available even after migration of the system, if applicable.

**9.1 Audit Log Structure**

- User Identification- Transaction ID
- Type of event
- Date and time of event
- Origination ID
- Authorization ID
- The name of affected data, system component or resources

**9.2 Audit Log Security**

All event logs must be collected in a centralized location or media that is protected from unauthorized access and difficult to alter via access control mechanisms, physical segregation, and/or network segregation. The viewing of such logs is to occur on a need only basis. The logs will be further protected by a change-detection software that alerts the Information Security Unit upon unauthorized access or if existing log data is changed. Logs for external-facing technologies such as wireless, firewalls, DNS, and mail, must be copied onto a log server on the internal LAN. Bank shall deploy Security Information and Event Management (SIEM) solution for monitoring critical servers/firewall/servers/application.

## CHAPTER 10 Data Retention and Disposal Policy

### 10.1 Data Retention

All confidential and sensitive data regardless of storage location, will be retained only as long as required for legal, regulatory and business requirement. All system and network audit logs must be retained for one year with ability of immediately restoring at least the last three month's logs for analysis.

### 10.2 Disposal Requirements

All restricted and internal electronic data not required to be retained as per legal, regulatory and business requirement must be removed from GIBL Systems using the approved method documented in this policy.

### 10.3 Disposal Process

Media containing confidential or sensitive data that should no longer be retained must be disposed of in a secure and safe manner as specified in disposal process:

- **Hard disks:** sanitize (7-pass binary wipe) or physically incapacitate platters.
- **Tape media:** degauss, shred, incinerate, pulverize or melt.
- **USB "thumb" drives, smart cards, and digital media:** incinerate, pulverize or melt.
- **Optical disks (CDs and DVDs):** destroy optical surface, incinerate, pulverize, shred or melt.
- **Hardcopies (paper receipts, paper reports, and faxes):** cross-cut shredded, incinerated, or pulped.

## CHAPTER 11 Network Infrastructure Security

Management of all Network firewalls and routers shall be combined effort of Network Administrator and the Information Security Unit.

### 11.1 Roles of Network Administrator

- Assure that changes to hardware, software, and security rules of firewalls and routers are approved Firewall Change Request Form.
- Document all firewall and router security rule changes
- After every change, review and update network diagrams to assure they accurately describe all connections to confidential or sensitive information, wireless networks, and critical network protection mechanisms (e.g., firewalls, IDS/IPS, anti-virus systems, access control systems, etc.).
- Enable audit logs on all security systems and perform daily monitoring of the logs.
- Provide Information Security Unit with read-only access to security audit logs.
- Report network security incidents to the Information Security Unit immediately upon discovery.
- Coordinate an appropriate response with Information Security Unit to mitigate security events.
- Keep backup for 3 consecutive rules of firewalls and routers and provide a copy of backup to Information Security Unit
- Maintain Inventory of Firewalls and Network Devices.

### 11.2 Roles of Information Security Unit

- Ensure that security rules applied to the firewalls and routers are sufficient to protect GIBL networks and corporate assets from external attacks and unauthorized access.
- Review all firewall and router security rule change requests for policy compliance
- Ensure that all ports/services allowed through the firewalls and routers are properly documented
- Ensure risky protocols, such as FTP, TELNET, POP3, IMAP, and SNMP, have undergone a risk assessment, have a current documented business need, and are secured as per documented security standard.
- Monitor Firewall and router security events to identify internal and external security incidents.
- Conduct semi- annually review of firewall and network devices.
- Conduct Vulnerability assessment and Penetration testing of Network Devices.

## CHAPTER 12 Remote Access

If access to any of the computing systems needs to be done remotely, adequate technologies must be used to guarantee that no risk is placed on GIBL network environment. In particular, the following must be followed:

- Technologies such as SSH, VPN or TLS v1.2 or above must be used for all administration.
- All remote access to the GIBL network involving public networks such as the Internet must be authenticated via a strong two-factor authentication scheme. This will be accomplished by using a password as one factor (something you know) and a unique token or certificate as the second factor (something you have).
- If there is a need to allow external access to a vendor or contractor, a maintenance window must be approved and scheduled ahead of time. The following process must be observed by the Network Administrator to connect and disconnect external entities:
  - Verify that the access request form has been properly completed and authorized by concerned department before allowing any access.
  - In case of uncertainty, contact the manager authorizing the connection to verify the authenticity of the authorization.
  - Allow access at the appointed time.
  - Monitor connection.
  - Disable access after the allowed time is over.
  - Monitor system performance after the connection to identify any anomaly.

## CHAPTER 13 Backup Policy

Although backup policy is related closely to the business continuity and disaster recovery policy (BCDR), since it protects against events that are relatively likely to occur, in practice it will be used more frequently than the BCDR. The purpose of this policy is to provide consistent rules for backup management to ensure backups are available when needed.

### 13.1 Data to be backed up

All data stored on the Firm's file servers, email servers, network servers, web servers, database servers, domain controllers, firewalls, and remote access servers need to be backed up. It is the user's responsibility to ensure any data of importance is moved to the file server.

### 13.2 Backup Storage

When stored onsite, backup media must be stored in a fireproof container in an access-controlled area. When moved offsite, a hardened facility (i.e., commercial backup service) that uses accepted methods of environmental controls, including fire suppression, and security processes must be used to ensure the integrity of the backup media.

All media that is transferred from one location to another should be logged as being transferred, by whom, where, and was it properly received, with signature from management.

The off-site storage location must be visited by Information Security Unit annually to confirm that it is physically secure.

### 13.3 Backup Method

Following backup method must be used for taking backup:

- a. **Full Backup** –Every time data backup is taken of full database irrespective of earlier backup.
- b. **Differential Backup**-Backup is taken only of data changed/modified since last full backup
- Increment Backup**- Backup is taken only of data changed/modified since last backup (last backup can be either full back up or increment backup)

### 13.4 Audit

All Back-up media must be classified according to Data Classification Policy prescribed on Information Security Policy. All back-up media should be assigned with unique tracking number and must be registered with the Information Security Unit for tracking prior to use. Quarterly inventories of all stored media will take place. The Information Security Unit will compare their list in use media with records at the storage facilities.

### 13.5 Restoration Procedure and Documentation

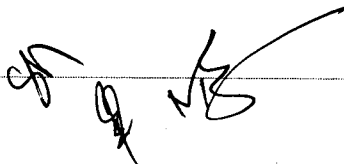
Approval from IT manager and concerned data owner shall be responsible for the data restoration. Information Security Unit shall be informed about the restoration procedure.

### 13.6 Data Destruction

All media that is no longer needed or has reached end-of-life must be destroyed or rendered unreadable so that no data may be extracted. Data destruction shall be as per Disposal process of Information Security Policy.

Me









## CHAPTER 14

**INCIDENT RESPONSE PLAN AND PROCEDURES**

A computer security incident is violation or imminent threat of violation of computer security policies, acceptable use policies, or standard securities that has significant potential to lead to the following:

- Negative Impact to the company's reputation.
- Loss of Intellectual Property or Funds.
- Inappropriate access to PII (Personally Identifiable Information) or customer data.

**14.1 Assembling Information Technology Incident Response Team (IRT)**

GIBL IRT shall act according to TOR for Incident Response Plan and Procedure. The following professionals need to be part of IRT to ensure encourage of specific incident –response plan.

- Chief Information Technology Officer (Head-IT)
- Information Security Officer (ISO)
- Chief Operating Officer (COO)
- Network In-charge
- Head Legal

**Steps for Incident Response Plan:**

- |          |   |
|----------|---|
| Step I   | Determine authority to call an incident                 |
| Step II  | Assign IRT responsibilities                             |
| Step III | Do not assign severity levels.                          |
| Step IV  | Establish communication procedures and responsibilities |
| Step V   | Gather Pertinent Information                            |
| Step VI  | Outline the Process                                     |
| Step VII | Review and test the plan                                |



## CHAPTER 15 Encryption Policy

All applicable mechanisms and systems on GIBL networks, whether managed by employees or by third parties shall meet encryption policy standard. Encryption keys must be protected from general access. Only approved custodians should be able to access the key components.

### 15.1 Key Access Authorization/ Custodian

Access to encryption key components will only be granted to those custodians specially requiring access due to their job function. Access shall be granted on prior approval from Chief Information Technology Officer based on their job description.

### 15.2 Split Knowledge and Dual Control

If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control. For example, requiring two or three key custodians, each knowing only their own key component, to reconstruct the whole key. No single custodian may know or have access to all components of an encrypting key. Applicable key management operations include, but are not limited to: key generation, distribution, change, storage and destruction.

### 15.3 Key Generation

Only strong encryption keys are to be used. Creation of encryption keys must be accomplished using a random or pseudo-random number generation algorithm. Industry best practices encryption methodologies should be used.

### 15.4 Key Distribution

Only custodians authorized by the Information Security Unit are allowed to retrieve key components from secure storage or to distribute keys. The encryption keys must never be distributed in the clear.

### 15.5 Key Storage

All data-encrypting keys must be stored encrypted in a secure location and in the fewest number of possible locations and forms. Clear-text backups of encryption key components must be stored separately in tamper-evident packaging in a secure location.

### 15.6 Key Changes

Information Security Unit must be involved in key changes and destruction. The situation where key changes is required are:

- Regular Key Rotation:** Normally, Key Rotation must be done at least a year.
- Suspicious Activity:** Keys must be changed if Information Security Unit finds suspicious activity of users.
- Resource change:** Key must be changed after the authorized person is changed.
- Technical requirement:** Due to questionable technical issues raised at the place where key was kept.

## CHAPTER 16 Usages Policy for Critical Information Assets/Technology

All users of critical information assets deployed in GIBL must follow this policy.

Critical Information Assets/ Technologies are:

- a. Remote access technologies
- b. Wireless technologies
- c. Removable electronic devices
- d. Laptops
- e. Tablets
- f. E-mail usage
- g. Internet Usage

Critical Information Assets/ Technologies shall be based on following guidelines/ role matrix defined.

- Laptop/Tablets Usage shall be as per **Laptop Usage Guidelines**. IT Support shall act accordingly.
- E-Mail usage shall be as per **E-Mail ID Guidelines**. IT support shall act according to E-Mail ID Guidelines.
- Removable Electronic Devices usage shall be as per **Removable Electronic Device Management Process**.
- Internet usage shall be based on **role matrix defined, documented and approved**. Network administrator must provide Internet Access usability based on approved role matrix.
- WI-FI access shall be based on role matrix documented and approved. Support Unit must provide WI-FI based on approved role matrix.

### 15.7 Key Destruction

Key not required must be disposed as per data retention and disposal Policy.

### 15.8 Email Transmission of Confidential Information

Restricted and Internal information is never to be sent through end-user messaging technologies such as e-mail, instant messaging, or chat.

## CHAPTER 17 Change Management Policy

The Change Control policy is designed to provide a managed and orderly method in which changes to the information technology environment are requested, tested and approved prior to installation or implementation. The purpose is not to question the rationale of a change, but to ensure that all elements are in place, there is no negative impact on the infrastructure, all the necessary parties are notified in advance and the schedule for implementation is coordinated with all other activities

### 17.1 Change Management Process

Change Management provides a process to apply changes, upgrades, or modifications to the environment. This covers any and all changes to hardware, software or applications. It also includes modifications, additions or changes to the LAN/WAN, Network or Server hardware and software, or any other environmental components such as electrical or cooling systems. The policy is in place to ensure that any change that affects one or all of the environments that GIBL relies on to conduct normal business operations are protected.

Changes to the environment arise from many circumstances, such as:

- User requests
- Hardware and/or software upgrades
- Acquisition of new hardware and/or software
- Environmental changes
- Business Operational schedule changes
- Unforeseen events
- Scheduled Periodic Maintenance

### 17.2 Emergencies

Emergencies exist only as a result of:

- An office is completely out of service,
- There is a sever degradation of service needing immediate action,
- A system/application/component is inoperable and the failure causes a negative impact
- A response to an emergency business need.

### 17.3 Scheduled or Planned Maintenance

Prior the commencement of any planned or scheduled maintenance, the “Change Management Form” (document name and number) must be completed and signed off by a supervising member of the IT Department. Information Security Unit shall be part of Change Control Final Management Approval Team.

**CHAPTER 18      Miscellaneous****18.1 Back- End Database Update Policy**

GIBL shall never practice updating database by accessing back-end directly. But, if it has to be done due to genuine business need and after risk assessment, it should be done as per approved role matrix defined based on nature, type, event and its criticality. All back-end database update shall be reported as exceptional and communicated to management team.