

**General Circular No 2024/ 03**

**2nd April 2024**

**ESTABLISHMENT OF INCIDENT & VULNERABILITY MANAGEMENT**

1. **With the objective of mitigating the risk from IT infrastructure incidents by providing practical guidelines on responding to incidents effectively and efficiently. Purpose of this process is to restore the normal service as quickly as possible and minimize the adverse impact on business operations.**
2. **Under this process all users must immediately report all IT incidents to the LCB Finance IT Department, whether confirmed or suspected. To report such incident a specific report form is introduced and a specimen of the report form is attached herewith. Branch users can report IT incidents using the telephone as well and in such case the IT department officer must take sufficient details from the reporting officer to fill the incident report and to resolve the Issue.**
3. **Specimen of the report will be made available in the LCB Finance intranet for downloading. Completed issue report should be emailed to** [**it@lcbfinance.lk**](mailto:it@lcbfinance.lk) **email address. If reporting the issue via telephone please use Extension 216, Ext 217 or Ext 215. Any incident to be reported after office hours please use these mobile numbers: 077-946 0956 or 077 066 8436.**
4. **Please refer attachment for the operational procedures that NEEDS TO BE FOLLOWED**

**This process will be effective form 3rd. April 2024.**

**Signed Signed**

**DEPUTY GENERAL MANAGER (IT) CEO / EXECUTIVE DIRECTOR**

**Attachment referred to in General Circular No 2024/03 of 2nd April 2024**

1. **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.**

1. **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.**

1. **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.**
     + 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.**

* + - 1. **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.**

* + - 1. **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.**
  + - 1. **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.**

* + - 1. **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.**

* + - 1. **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.**

* + - 1. **Incident resolution**

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

* + - 1. **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 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.**

**End of Document**