Approval’s page

|  |  |  |  |
| --- | --- | --- | --- |
|  | Done by | Reviewed by | Approved by |
| Job title |  |  |  |
| Date \ Signature |  |  |  |

Information security incident management policy and procedures

**1 Policy Statement**

* Incident Management policy shall enable the response to a major incident or disaster by implementing a plan to restore the critical business functions of Al Qarib. The number of computer security incidents and the resulting cost of business disruption and service restoration rise with the increase in dependence on IT-enabled processes. Implementation of sound security policies, blocking of unnecessary access to networks and computers, improvement in user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce such risks and decrease the cost of security incidents.

**2 Purpose**

* The purpose of the incident management policy is to provide company-wide guidance to employees on the proper response to, and efficient and timely reporting of, computer security-related incidents, such as computer viruses, unauthorized user activity, and suspected compromise of data. It also addresses non-IT incidents such as power failure. Further, this policy provides guidance regarding the need for developing and maintaining an incident management process within Al Qarib.

**3 Scope**

**3.1 Employees**

* This policy applies to all Employees, Contractors, and Third-Party Employees, who use, process, and manage information from individual systems or servers.

**3.2 Documentation**

* The documentation shall consist of Incident Management Policy, and related procedures.

**3.3 Document Control**

* The Incident Management Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purposes.

**3.4 Records**

* Records being generated as part of the Incident Management Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

**3.5 Distribution and Maintenance**

* The Incident Management Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the system administrators.

**4 Privacy**

**The Incident Management Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.**

**5 Responsibility**

* The Incident Management Policy shall be implemented by the designated personnel. The primary responsibilities associated with incident management are to identify and respond to suspected or known security incidents, contain or limit the exposure to loss, and mitigate (to the extent practical) the harmful effects of security incidents. The IT department will manage incidents at the company level, an IT department security representative shall be assigned to facilitate the handling of security incidents. The nature of the incident may require the assignment of staff from other divisions/offices. In all cases, top management shall be informed of the incident and the steps recommended or taken to mitigate the incident.

**6 Policy**

The top management shall ensure that:

1. Incidents are detected as soon as possible and properly reported.
2. Incidents are handled by appropriate authorized personnel with ‘skilled’ backup as required.
3. Incidents are properly recorded and documented.
4. All evidence is gathered, recorded and maintained in the Security Incident Reporting form that will withstand internal and external scrutiny.
5. The full extent and implications relating to an incident are understood.
6. Incidents are dealt with in a timely manner and service(s) restored as soon as possible.
7. Similar incidents will not recur.
8. Any weaknesses in procedures or policies are identified and addressed.
9. All incidents shall be analyzed and reported to the designated officer.
10. Learning from the incidents are recorded.

The policy shall apply throughout the company, including information resources, data stored and processed on those systems, data communication and transmission media, and personnel who use information resources.

**7. Implementation**

This shall develop, maintain and implement an incident management and response plan that addresses information technology security incidents. The following paragraphs specify the incident management plan requirements. These requirements shall be in compliance with relevant State and policies and standards.

1. **Incident Management Training:** This shall provide incident management training to the Divisions/Offices on how to identify and report security incidents.
2. **Identifying and Prioritizing Types of Incidents:** This will develop and maintain guidelines for identifying and prioritizing security incidents. The Divisions/Offices or their affiliated staff designated by agreement or assignment shall evaluate the potential for the occurrence of certain types of incidents. All security incidents shall be classified by severity level and type. The following five event severity levels as defined in the ITS Incident Response Standard shall be used for classification purposes. In addition, each incident shall be identified as to type: email, hacking, virus/worm, inappropriate use, social engineering and other.
3. **Incident Monitoring:** The Al Qarib shall develop and maintain guidelines on how to monitor for security incidents. The Divisions/Offices or their affiliated staff designated by agreement or assignment, as part of their risk management program, shall continuously monitor for security incidents (both physical and Technical – related incidents) according to the guidelines listed above.
4. **Incident Detection:** The IT department shall develop and maintain enterprise-wide procedures for collecting, analyzing, and reporting data. The integrity of all data relating to criminal acts must be preserved as possible evidence and collected.
5. **Incident Reporting:** The IT department shall define the basic procedure to be followed for reporting incidents. The procedure shall be expanded upon by the Divisions/Offices as necessary to include the internal communications and escalation procedures that will be used. Security incidents classified as level 3, 4, or 5 shall be reported to the top management and the related department within a period of 24 hours from the time the incident was discovered and submit an incident report to take the suitable action.
6. **Organization Protocols:** Security incidents may occur across network boundaries. The IT department shall define the protocols for handling these incidents and the contacts between Divisions/Offices, state agencies and outsourced entities.
7. **Impact Assessment:** The IT department shall evaluate the impact of security incidents. Assessments may be required at various stages of the incident life cycle to assist management in deploying the proper risk management procedure.
8. **Documentation**: All security incidents shall be thoroughly documented by the Divisions/Offices with as much detail as possible to describe the incident, time discovered and impacted area for subsequent investigation. The incident report shall indicate who was notified and what actions were taken.
9. **Record Retention:** Divisions/Offices shall maintain the incident logs and corresponding documentation for a minimum of one year following the discovery of an incident or until an investigation is completed. Incident logs should be stored in a secure location.
10. **Post-Incident Analysis:** It is necessary to amend the risk register, assess the risk that occurred, and put preventive procedures to avoid such risks.

Related forms \ documents:

1. Incident Reporting Form for breaches of security or confidentiality
2. Risk Register