|  |  |
| --- | --- |
| **Document Name** | **Incident Management Policy** |
| **Version** | **0.3** |
| **Last Updated by** | **Anjaly T A** |
| **Approved By** | **Inderjit Singh Bedi** |
| **Released on** | **07-09-2022** |

Contents

[1 Policy Statement 3](#_Toc113467977)

[2 Purpose 3](#_Toc113467978)

[3 Scope 3](#_Toc113467979)

[4 Privacy 4](#_Toc113467980)

[5 Responsibility 4](#_Toc113467981)

[6 Policy 4](#_Toc113467982)

[7. Implementation 5](#_Toc113467983)

### **1 Policy Statement**

Incident Management policy shall enable response to a major incident or disaster by implementing a plan to restore the critical business functions of Xtracap Fintech. The number of computer security incidents and the resulting cost of business disruption and service restoration rise with 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 organization-wide guidance to employees on 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 Xtracap Fintech.

### **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 purpose.

#### **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 CISO and 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 CISO / 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 Xtracap Fintech’s’s Division will manage incidents at the facility level. Where facilities are leased or ITS support is provided by an affiliate(s), a Xtracap Fintech’s Division/Office 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, division/office management shall be informed of the incident and the steps recommended or taken to mitigate the incident.

### **6 Policy**

The organizational 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. The risk to company’ss reputation through negative exposure is minimized.
10. All incidents shall be analyzed and reported to the designated officer(s).
11. Learning from the incidents are recorded.

The policy shall apply throughout the organization, 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 CISO 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 ITS – related incidents) according to the guidelines listed above.
4. **Incident Detection:** The CISO 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 will be collected using generally accepted forensic procedures. The forensic procedures to be followed will be developed and disseminated by the CISO.
5. **Incident Reporting:** The CISO 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, or 4 shall be reported to the CISO and the division/office information security official within a period of 24 hours from the time the incident was discovered. The CISO is responsible for reporting the incidents to ITS and the Assistant Secretary for the OPP and Compliance within 24 hours of receiving the report. The Assistant Secretary for OPP and Compliance will be responsible for letting appropriate departmental staff know about the issue. The division should not report directly to ITS, as it could result in duplicate incidents being reported. A manual form may be completed and forwarded to the division/office information security official for processing. An incident reporting template is Available with the CISO and IT Manager. Reporting of security instances classified as level 2 or greater should be reported, at a minimum, to the division/office security official. Division/office specific procedures may require all levels of security incidents to be reported to the CISO. If there is a question regarding classification level, the division/office security official should consult with the CISO.
6. **Security Incident Response Team (SIRT):** The CISO shall establish and utilize an SIRT. The CISO will work with the Divisions/Offices to develop a cross-functional incident response team that will handle a variety of incidents. The roles and responsibilities of the team members will be clearly defined.  The SIRT shall be adequately staffed and trained to handle the incident(s). Since incidents may be far-reaching, requiring expertise or authority that does not reside within a division/office, the SIRT may include outsourced vendors, internal and external entities, as well as other key facility/agency personnel.
7. **Organization Protocols:** Security incidents may occur across network boundaries. The CISO shall define the protocols for handling these incidents and the contacts between Divisions/Offices, state agencies and outsourced entities.
8. **Impact Assessment:** The CISO 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 strategy.
9. **Incident Handling and Escalation Procedures:** The CISO shall develop and maintain the primary procedures for handling the containment, eradication and recovery aspects of incidents and the guidelines for development of an escalation procedure. The Divisions/Offices shall develop escalation procedures that are tailored to their individual circumstances.
10. **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. The CISO may be called on to assist in the documentation process.
11. **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.
12. **Post-Incident Analysis:** The post-mortem analysis provides feedback to improve the existing process and its related procedures. Following actions taken to resolve each security incident, an analysis shall be performed by the CISO and the impacted division or office, with assistance of their affiliated staff designated by agreement or assignment, to evaluate the procedures taken and what further steps could have been taken to minimize the impact of the incident.
13. **Emergency Planning:** If an incident occurs that impacts the safety of citizens, personnel, facilities or results in a situation where agency services are interrupted for an extended period of time, the incident may be declared an emergency. The KDCCCISO shall work with the Disaster Response Team to provide guidelines regarding the criteria for identifying an emergency and notification procedures. The Divisions/Offices shall develop the appropriate procedures for identifying and declaring emergencies using the established Business Continuity and Disaster Recovery Policy.
14. **Media Relations:** Serious security incidents that are likely to result in media attention shall be reported immediately to the Department of Public Affairs Office.

8. Incident Management SLA

|  |  |  |  |
| --- | --- | --- | --- |
| Response Time\* | Resolution Time | Priority | Priority Criteria for Escalations. |
| 15 min | 1 Hr | P1- Urgent | Blocking production issues / Production Incidents/Software attacks/ theft of intellectual property/Information extortion |
| 1 Hr | 8 Hrs | P2- High | Support & Security incidents related to Customer Onboarding |
| 8+ Hrs | 24 Hrs | P3- Medium | Backend Support / Security issues due to Manual Processes/ power outages/ Damage to properties |
| 24+ Hrs | 2 Week | P4- Low | Low priority security Issues |