TechSture Technologies

Incident Reporting Policy

Document No – TT-ITP/08

Document Release Note

Document Version	1.0	**Release Date**	

Prepared By	**Verified By**	**Approved By**

Document Revision History

Version	Date	Change Description	Modified By	Reviewed By	Approved By
1.0					

1.1 Purpose

The purpose of Incident Management policy is to restore normal service operations as quickly as possible. It also ensures that the best possible levels of service quality and availability are maintained. This policy also covers problem management

1.2 Scope

This procedure is applicable to incident reporting for information assets.

1.3 Policy

A well-defined and systematic approach shall be followed to respond to reported, observed or suspected information security incidents. Organization shall form an **incident management team** to deal with Co-ordination, Communication, reporting Assessment, Investigation & Recovery and closure of Information security incident. **Appropriate controls & mechanism** shall be deployed to monitor, detect, prevent or mitigate and recover from incidents. Management shall develop and review alternate communication channels to reduce stress in case of an actual incident.

1.3.1 Incident Identification/Classification

An incident is an unplanned interruption to an IT Service or reduction in the Quality of an IT Service, breach of data integrity, Failure of any Item, software or hardware, used in the support of a system that has not yet affected service is also an Incident. For example, the failure of one component of a redundant high availability configuration is an incident even though it does not interrupt service.

An incident occurs when the operational status of a production item changes from working to failing or about to fail, resulting in a condition in which the item is not functioning as it was designed or implemented. The resolution for an incident involves implementing a repair to restore the item to its original state. Incident events can be caused by but not limited to:

- Unauthorised physical or logical access
- Human error
- Uncontrolled System change
- System Loss or failure
- Loss or theft of Physical asset
- Malfunction of software or hardware
- Vulnerability in System
- Virus or malware activity
- Inaccurate business data
- Denial of service or access
- Breach of data or confidentiality

After reviewing incidents and other parameters, it can be further classified by following process.

- Log review for incident management
    - Anti-Virus Patterns shall be checked for updates on Servers and end clients and logs shall be reviewed on the daily basis to identify infected systems.
    - Server Security Logs review – On Daily basis IT Department shall review the Server Security logs for any violations.
    - Firewall & IDS/IPS Logs review – On daily basis IT Department shall review the Firewall & IDS/IPS logs for any attacks for checking if the attack successfully entered or was denied and follow subsequent Incident management procedures
    - System security Logs will be maintained for incident investigations and should be retained for 3 years.
    - Database access logs for all production servers where Techsture is providing maintenance and internal IT development servers
    - Logs of Other Tools and technologies shall be maintained for a month for correlating and identifying the event as True positive.
    - Network access logs

- Impact shall be determined by the degree of loss of Confidentiality, data loss/modification, Integrity and Availability of affected resource (Information and its processing device) of the organization.
- All Incidents shall be prioritized based on severity and impact of the incident. All the incidents shall be classified as confidential and prioritized as below.
    - **Low Priority** Incident is the one which would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.
    - **Medium Priority** Incident is the one which would cause a moderate disruption in the business, minor legal ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.
    - **High Priority** Incident is the one which would cause an extreme disruption in the business, cause major legal or financial ramifications, violate the privacy of Customer, Client information, threaten the health and safety of a person, processor business and/or result in any business, financial, or legal loss or direct, negative impacts on the finances, operations, or reputation of the organization. All incidents that occur in the "Confidential Data Processing Unit" will be treated as high priority incidents.

1.3.2 Incident Reporting

All users with access to TechSture resources shall report observed or suspected information security incidents to their department supervisor & Technology team with copy of ticket logged on below helpdesk portal.

http://portal

The incident response team shall record the incident and depending on the incident, incident reporting form should be filled by IT Department. Report shall be generated and sent to the respective department head security Team or Clients if required. The incident shall be classified as per the criteria detailed above.

1.3.3 Incident Analysis and Response

- The appropriate technical resources from each site shall be responsible for monitoring such that any damage from security incident is repaired or migrated and that the vulnerability to a threat is eliminated or minimized where possible.
- Appropriate personnel/team members shall be deputed by the respective department for doing a preliminary analysis to ascertain the cause and extent of damage caused by the incident.
- The Members shall be responsible for initiating, completing, documenting and communicating the incident investigation.
- Based on The Impact and severity of Incident, Technical Director shall be responsible for notifying the Management Team and initiating appropriate incident management action including restoration by getting assistance from appropriate TechSture officials from Admin, Operations, Finance, HR and IT Confirmed and true positive Incidents shall be reported to Management, Clients and appropriate Department as per respective Incident Reporting Call tree.
- IT Department and Admin team shall be responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- All the systems should be immediately excluded from the network as soon as the abnormal behaviour reported
- In case where law enforcement is involved, IS Officer shall act as liaison between laws Enforcement and TechSture.
- In case where law enforcement is not involved, TechSture Management Team shall recommend relevant disciplinary actions.

1.3.4 Incident Recovery/containment

Containment of an incident is critical to ensure that it does not propagate, change or disappear before it can be dealt with. The steps that need to be performed, depends on the nature and impact of the incident and may include some or all the following:

- Based on data available and level of criticality of incident, team shall send out alerts to departments which may possibly be affected by the incidents.
- Additional monitoring mechanisms shall be deployed for a short duration of time after recovery to ensure that all incident affected activities have resumed.
- Appropriate recovery plans and co-ordination mechanism for business continuity shall be developed and followed to recover from Incidents that may include but not limiting to

    - Removing the vulnerability/weakness/malicious content.
    - Securing the system from the effects of the incident.
    - Evaluating whether certain actions are likely to result in proportion to their cost and risk, those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
    - Collecting evidence where criminal prosecution, or Organization's disciplinary action, is contemplated.
    - In addition, Security team will collect statistics concerning incidents which occur within or involve the affected environment, and notify the stakeholders as necessary to assist it in further protection of resources.

1.3.5 Incident Prevention/Post Analysis

- Preventive measures as applicable shall be defined & implemented by security team to prevent re-occurrence of similar incidents.
- Based on the identification of control weaknesses, identified improvement opportunities, Security team shall make necessary changes (if required) to appropriate policies procedure and standard.

1.3.6 Security Incident Management Awareness

All employees, contractors, subcontractors, agencies, consultants, business partners, visitors, Service providers and third parties shall be made aware of the procedures to ensure they are aware of information security threats and concerns encountered during their normal work. TechSture will develop and make available Security instructor led training and update training as required and notify Departmental heads and Management of significant updates to the Security Awareness training.

1.4 Records

Incident reporting registration.

1.5 Effective Measures

Number of incident reported.