Information Technology Incident Management Policy

ITP Number	**Effective Date**
ITP-SYS012	Maret 23, 2024
Category	**Supersedes**
IT Security Systems Management	None
Contact	**Scheduled Review:**
it@pttuntex.com	None

Policy Summary

As a means of organizing and directing the Tuntex's response to observable threats to its Information Technology ("IT") Resources and systems, this policy establishes roles, responsibilities, and procedures for reporting and managing IT Incidents. Written directions for responding to IT Incidents increase Tuntex Company's ability to mitigate threats, minimize risk of loss or destruction of Company information, and help to restore services more quickly when events do occur. All Tuntex Community Members that use Tuntex IT Resources are advised to immediately report any IT-related concern to Information Technology Services.

Purpose

Responding to IT-related threats or challenges is essential to maintaining the confidentiality, integrity, and availability of the Tuntex's IT Resources.

Entities Affected By This Policy

- All unit that interact with Tuntex Information or Tuntex IT Resources
- External entities granted access to Company Information
- Information Technology Services

Who Should Know This Policy

- All Tuntex Community Members that use Tuntex IT Resources
- Tuntex Management
- External agents granted access to Tuntex Information
- Information Technology Services Leadership Team
- Employees/Staff

Definitions

Information Technology ("IT") Resource: any computer, server, communication or mobile device, or electronic data, data storage, transmission or control device that is owned and/or operated by the Tuntex Company, used to conduct Tuntex business, or connected to the Tuntex's IT networking or communication systems regardless of ownership, location, or access method. These resources are referred to herein as "IT Resources.

IT Incident: an observable or recognizable occurrence that threatens or causes adverse consequences for the confidentiality, integrity, or availability of the Tuntex's IT Resources.

Major IT Incident: an IT Incident of significant scope or scale that affects large numbers of Tuntex IT Resources and Tuntex Community Members, or that results in extended downtime of IT services.

Sensitive Information: all information that should remain private or confidential as designated by the Tuntex Company or as required by law, including, but not limited to, management and employee conduct records, ID numbers, credit card or banking information, regulated research data, and health care provider records. Sensitive Information includes, but is not limited to, buyer data and vendor data.

Tuntex Information: all written or verbal data or information that the Tuntex company or its employees, management, or designated affiliates or agents collect, possess, or have access to regardless of the medium on which it is stored or its format.

Tuntex Community Member: all Tuntex employees, management, affiliates, contractors, consultants, agents, and volunteers wherever located.

Policy

A. Applicability

This policy applies to all Tuntex Community Members and other persons who access or use Tuntex Information, including third-party individuals or entities. Additionally, this policy applies to all Tuntex IT Resources, all applications or data contained on these devices or systems, and all other devices, including privately owned devices, that connect to the Tuntex's information networks or data storage systems.

B. Examples

A partial list of potential IT Incidents (or Major IT Incidents depending on scale) includes:

- Unauthorized access of Tuntex IT Resources, systems, or Tuntex Information
- Violation of the Appropriate Use of IT Resources policy
- Violation of the Information Security policy
- Unauthorized changes to Tuntex production systems
- Loss, theft, or damage to Tuntex IT Resources
- Unexpected disruption or IT system unavailability
- Compromised user accounts
- Unauthorized disclosure of Sensitive Information
- Malicious attacks propagated by computer viruses, malware, ransomware, or phishing schemes

- Zero-Day Vulnerabilities
- Third party breach or incident

C. Reporting

Tuntex Community Members who use the Tuntex's IT Resources are strongly encouraged to immediately report suspected IT Incidents or Major IT Incidents to Information Technology Services ("ITS"). ITS personnel shall utilize the Tuntex Company incident tracking system, for all reporting and incident documentation. Reports of actual or suspected IT Incidents or Major IT Incidents should be submitted as appropriate to the following:

- ITS Service Desk
  - ✓ itsupport@pttuntex.com
  - ✓ https://pttuntex.com/

D. IT Incident Management

The IT Div Head, in collaboration with the ITS team, shall establish and revise as necessary or appropriate the Tuntex's IT Incident and Major IT Incident management protocols, to be maintained within the ITS system of record, that will provide for the following:

1. Identification and Classification – the reported incident shall be analyzed and details confirmed to determine if a reported incident does in fact constitute an IT Incident or a Major IT Incident. This classification will assist with determining the proper response procedure and the selection of appropriate personnel for managing the response.

2. Containment and Eradication – the systems affected or implicated shall be isolated and/or further monitored to prevent wider or additional negative impact. Compromised systems will be immediately isolated from the network. Compromised user accounts that pose a threat will be blocked or isolated from the network.

3. Recovery and Restoration – once blocked systems are secured and threats eradicated, continued monitoring, logging, and auditing of activity will be implemented when blocked systems are re-introduced into the network. All significant findings will be documented, including analysis and remediation steps.

4. Response Team Review and Lessons Learned – post-incident activities will include debriefing meetings, review of incident handling procedures, and lessons learned discussions. Edits and republishing of procedures will be based on the debriefing meetings.

E. Training and Testing

ITS leadership shall ensure appropriate training of ITS team in effective IT Incident mitigation and response, consistent with the requirements of this policy. Testing of IT Incident response capabilities and proficiencies shall occur no less than annually using checklists, tabletop exercise, simulations, meetings, or comprehensive scenario-based exercises. Training and testing shall include lessons learned from previous IT Incident management activities. IT Incident-related training and testing shall focus on

improving the ability to respond effectively to a real event while continually identifying areas for growth and improvement. In the event actual incidents have occurred during the year, they may serve as one kind of training and testing, provided the protocols were followed and a full assessment and lessons learned phase takes place.

Information Security Awareness training is required of all Tuntex management, employees, staff, and other Authorized Users of Tuntex Information or IT Resources.

RESPONSIBILITIES

Head Information Technology: ensure that appropriate and auditable IT Incident management procedures are in place; has ultimate responsibility for the IT Incident management program.

Information Technology Services: maintain management procedures for IT Incidents and Major IT Incidents; design and participate in IT Incident training and testing exercises; respond to and manage IT Incident reports and responses.

Tuntex Community Members: promote the implementation of this policy within their respective areas of responsibility or jurisdiction and comply with the Appropriate Use of Information Technology Resources policy.

PROCEDURES

Information Technology Incident Response Procedure

Tuntex IT Division

Signature_____Annual Review Date _____