Threat and Vulnerability Management Policy

ITP Number	**Effective Date**
ITP-SYS013	Maret 23, 2024
Category	**Supersedes**
IT Security Systems Management	None
Contact	**Scheduled Review:**
it@pttuntex.com	None

Policy Statement

The Tuntex Company must maintain a threat and vulnerability management program to identify and remediate information security vulnerabilities.

Reason for the policy

To adequately protect the data and services entrusted to the company by the public. It is necessary to identify and remediate vulnerabilities within State IT systems. Monitoring for threats, vulnerabilities, and advisories along with vulnerability scanning and penetration testing identify security weaknesses within systems and allows for prioritization of resources to address the most critical areas. Timely remediation of vulnerabilities is critical to maintaining the availability, confidentiality, and integrity of State data.

Scope

This threat and vulnerability management policy applies to all systems, people and processes that constitute Tuntex information systems, including staff, supervisors, managers and Tuntex management, and third parties with access to Tuntex's information technology assets and called hereinafter as Tuntex Workforce.

Roles & Responsibilities

- Employees, Vendors, and Contractors
    - Be aware of and follow relevant information security policies, standards, and procedures
    - Ensure information security is incorporated into processes and procedures
    - Ensure contract language with contractors and vendors includes required information security controls

- Consult with information security staff on the purchase and procurement of information technology systems or services
- Contact information security staff or email itsupport@pttuntex.com with questions about the information security policies, standards, or procedures. Or Check on Tuntex's Customer relationship management (CRM) – Tuntex Redmine: IT Policies and Guidelines

- Supervisors, Managers and Management

Policy Content

1. Vulnerability and Patch Management Plan

A vulnerability and patch management plan must be created, implemented, maintained, and enforced at Tuntex Company.

- This plan must detail Tuntex's vulnerability and patch management program, including the implementation of mechanisms to timely obtain information about technical vulnerabilities of information systems, the evaluation of the Tuntex's exposure to such vulnerabilities and the implementation of appropriate safeguards to address the associated risk

- The plan must include supporting activities such as training and reporting metrics for effective implementation of the vulnerability and patch management program

- The plan must include roles and responsibilities of teams/roles for accomplishing all the activities of the vulnerability management program in a timely and effective manner

2. Create/Update a System Inventory

ITS must create a system inventory of IT resources in scope for the vulnerability management program to determine which brand, model and version of hardware equipment, operating systems, database, system, web server and software applications are used within the company.

System inventory must be updated on an annual basis or whenever changes occur to IT resources to ensure that all the IT resources are covered in Tuntex's vulnerability management program.

3. Monitor for Vulnerabilities, Remediations, and Threats

ITS must monitor security sources for vulnerability announcements, patch and non-patch remediations, and emerging threats that correspond to the Tuntex IT resources within the system inventory.

- ITS must establish procedures to obtain copies of the software updates electronically when they are issued by the vendor

- ITS must utilize authorized resources such as system vendor websites, third-party mailing lists and newsgroups, vulnerability management databases, and different tools for tracking the latest vulnerabilities

In addition to the regular application of vendor-supplied software updates, ITS must conduct regular vulnerability scans at least monthly, and a penetration test assessment on critical infrastructure and systems at least annually. The purpose of this assessment is to identify existing vulnerabilities in systems that could be exploited by an attacker.

- The monthly vulnerability scans may be carried out in-house or by an external company or a combination of both. Those vulnerability scans should cover all the internal and external facing assets on the production network

- The annual penetration test must be commissioned as required, using external qualified specialists as part of a carefully planned exercise, The plan must address the scope of the assessment, the methods to use, and the operational requirements, in order to provide the most accurate and relevant information about current vulnerabilities, without affecting the operation of the company

4. Prioritize Vulnerability Remediation

ITS must prioritize the order and scheduling in which the company addresses vulnerability remediation.

The scheduling of the installation of updates will depend upon several factors including:

- The criticality of the systems being updated

- The expected time taken to install the updates (and requirements for service outages to users).

- The degree of risk associated with any vulnerabilities that are being mitigated by the updates:

    - ✓ Tuntex must evaluate and assign a rating to each vulnerability as critical, high, medium, low, informational, or trivial.
    - ✓ Coordination of the updating of related components of the infrastructure.

- Dependencies between updates.

ITS must prioritize treatment of vulnerabilities based on their risk rating. Vulnerabilities with rating critical or high must be treated foremost. If patching is required for the vulnerability remediation, Tuntex must comply with below minimum service levels.

Vulnerability Risk Rating	Service Levels
Critical	Less than 3 days
High	Less than 7 day
Medium	90 days
Low	180 days

All the exceptions to this rule must be approved by authorized personnel, based on the risk acceptance process.

An updated release plan must be created and maintained to keep track of when various systems will be updated, taking into account the factors listed above. The plan must be managed through the change management process.

5. Create/Maintain Vulnerability Database

ITS must maintain a database of vulnerabilities gathered from multiple sources that require remediation and/or patching steps that need to be applied to Tuntex systems.

- All must include vulnerability information, vulnerability analysis for prioritization, and vulnerability remediation plan.

6. Conduct Testing of Remediations

All the remediations must be tested before deploying the changes to Tuntex systems. Failed remediations must be further examined for resolution.

7. Inform System Administrators and System Owners

All the vulnerabilities and respective remediation information must be informed to all the affected users, including system administrators, system owners, and end users.

8. Deploy Vulnerability Remediations

Only successfully tested vulnerability remediations must be deployed into production. Vulnerability remediation activities typically include security patch installation, configuration adjustment and/or software removal.

Where security patch installations and configuration changes are recommended to mitigate the vulnerabilities, these must be sent through the company change management process so that appropriate controls are in place for testing, risks assessment and backout.

9. Verify Vulnerability Remediation

ITS must verify systems for vulnerability remediations.

Successful remediation of vulnerabilities must be tested through network and host vulnerability scanning, checking patch logs, penetration tests, and verifying configuration settings.

10. Vulnerability Management Training

ITS must implement a training program for all participating team members on how to apply vulnerability remediations and best practices for effectively implementing the vulnerability management program, based on their roles in this process.

11. Vulnerability and Patch Management Metrics

ITS must consistently measure the effectiveness of its vulnerability and patch management program utilizing 'vulnerability and patch management metrics' and apply corrective actions as necessary.

On a monthly basis, these security metrics must be presented to the Information Security Governance Committee.

PROCEDURES

Threat and Vulnerability Management Policy

Tuntex IT Division

Signature_____Annual Review Date _____