[Insert Company Name and Logo]	
Title: IT Asset Management	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose

This procedure outlines the process to inventory and manage Information Technology assets across the enterprise. It is critical to keep asset controls up to date to ensure computer equipment and systems, along with its location are inventoried correctly. Equipment that is lost or stolen frequently carries sensitive data. Proper asset management methods and protocols provide documentation that can be used for recovery, replacement and/or insurance purposes.

Scope

This policy applies to all employees and other members of the workforce (whether paid, volunteer or contractor) working in all facilities under the organization's ownership. This policy also applies to the following activities:

1. Receiving a new physical IT asset
2. Transferring a physical IT asset
3. Migrating a virtual machine
4. Detecting, preventing, and responding to incidents
5. Continuously monitoring for unapproved hardware and software
6. Continuously monitoring for vulnerabilities and applying corporate-approved patches/updates

Mobile devices are not included in the scope of IT asset management unless those devices are also owned/controlled by the enterprise.

Definitions

<u>IT Asset</u>: Any company-owned hardware, software or network used to collect, process, maintain, transmit and/or disseminate information for daily business processes and activities.

<u>IT Asset Management</u>: Proper management of all financial, contractual and inventory functions of the IT Assets, both hardware and software, on premises or cloud based.

<u>Digital Asset Management</u>: Proper management of all intellectual property stored on company-owned devices in electronic media form and other business-related information produced by the company.

<u>Software Asset Management</u>: Proper management, control and cybersecurity of company-produced software and the purchased licenses for third-party software.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

Policy

[insert company name]'s Security Officer shall implement IT asset management policies and procedures for identifying and tracking all IT hardware and software owned/controlled and used by the enterprise by implementing the following security controls:

1. Establishing access control policy
2. Continuous monitoring and tracking of assets connected to a network
3. Event auditing
4. Anomalous activity detection and reporting
5. Vulnerability scanning

Users are routinely assigned or given access to IT equipment in connection with their official work duties. This equipment belongs to [insert company name] and must be immediately returned upon request or at the time an employee is separated from the organization. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the organization. Should IT equipment be lost, stolen, or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The organization has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

Procedures for IT Asset Management

1. Inventory of hardware, software, and data assets, including all system components (e.g., network address, machine name, software version, and data stored, processed, and/or transmitted) is required to be maintained at a level of granularity deemed necessary for tracking and reporting. Each individual IT asset must be identified and located and placed in an asset management system that makes it easy to quickly find and may be called up as needed. This inventory system should be automated where technically feasible.

2. All IT hardware, software, and data assets must be assigned to a designated business unit or individual. This includes data centers, software, hardware, mobile and cloud assets, networks, employee or user workstations, and any other business technology.

3. IT asset-related documentation must be organized and maintained for the entire life cycle of the IT asset. This includes proof of purchases, software licenses, certificates of authenticity, date of retirement of asset and any other relevant documentation.

4. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

Workforce members are responsible for reporting any suspected or known discrepancies or changes in IT hardware or software, attempts to attach unauthorized devices to the network or installation of unauthorized software onto any company-owned device to the Security Officer as soon as discovered.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

The Security Officer, upon notification of a suspected or known change, loss or theft of company-owned IT hardware or software, shall take immediate action to contain the incident and minimize damage to any sensitive or protected information and to our organization’s electronic systems that contain sensitive or protected information.

The Security Officer shall document all IT equipment incidents and actions taken to minimize harmful effects that are known to the organization in a written or electronic format *IT Incident Report* that is appropriately backed up. The *IT Incident Report* shall be maintained for X years.

The Security Officer is responsible for organizing, managing and maintaining IT asset-related documentation for the entire life cycle of the IT asset. This includes proof of purchases, software licenses, certificates of authenticity and any other relevant documentation.

The Security Officer is responsible for managing the secure disposal of outdated or broken IT assets. This includes data backups, information security, relocating software and mitigating any risks associated with IT asset disposal.

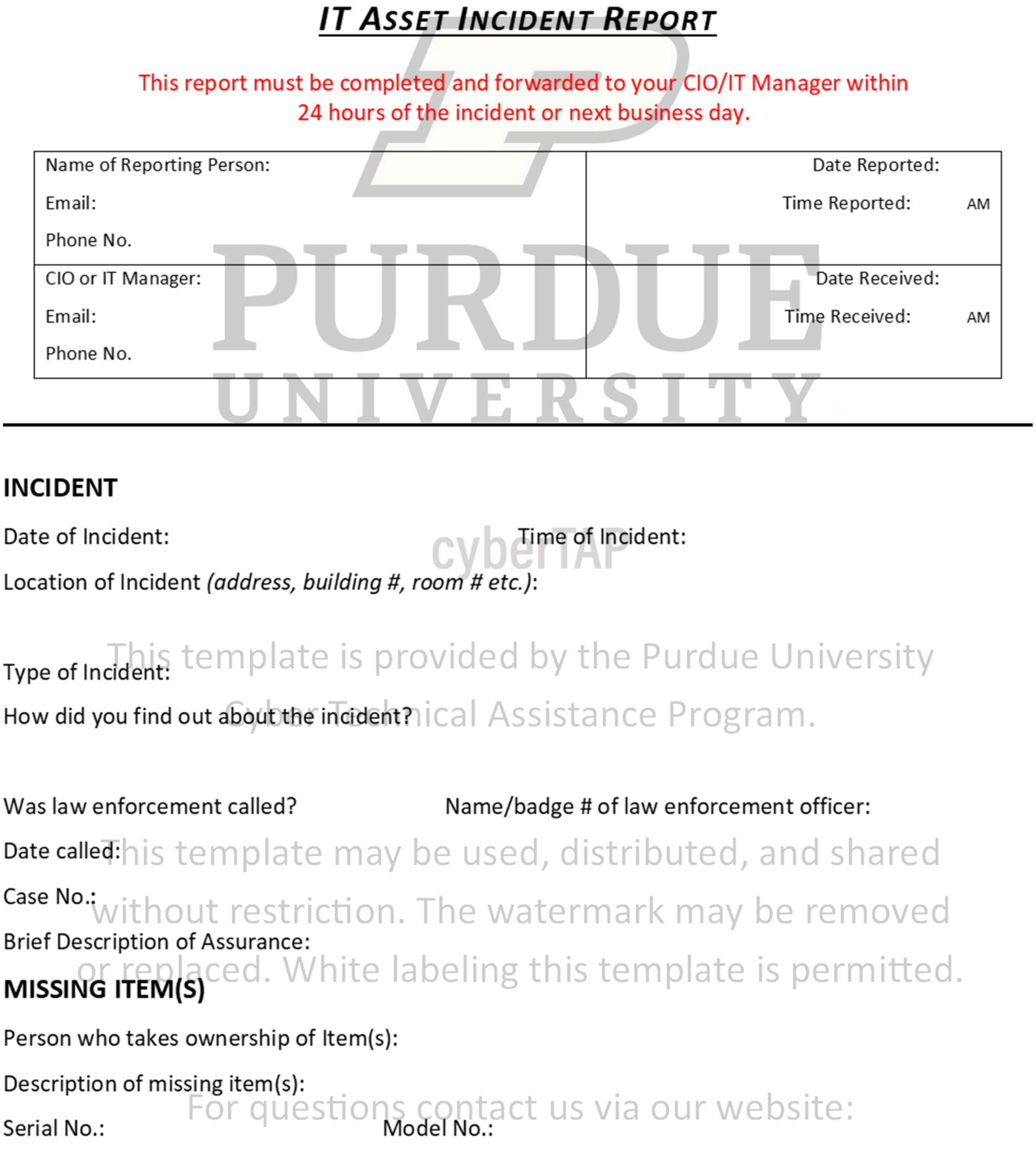
Violation: Employees who violate these policies and procedures are subject to discipline up to and including termination.

Attachments: Appendix A: [Reporting form for cybersecurity incident response]

Related Policies: Mapping Organizational Communication and Data Flows
Cataloging External Information Systems

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

Appendix A- [the form below is a placeholder only]



IT ASSET INCIDENT REPORT

This report must be completed and forwarded to your CIO/IT Manager within 24 hours of the incident or next business day.

Name of Reporting Person:	Date Reported:
Email:	Time Reported: AM
Phone No.	
CIO or IT Manager:	Date Received:
Email:	Time Received: AM
Phone No.	

INCIDENT

Date of Incident: Time of Incident:

Location of Incident *(address, building #, room # etc.)*:

Type of Incident:

How did you find out about the incident?

Was law enforcement called? Name/badge # of law enforcement officer:

Date called:

Case No.:

Brief Description of Assurance:

MISSING ITEM(S)

Person who takes ownership of Item(s):

Description of missing item(s):

Serial No.: Model No.:

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

DATA (RECORDS) CLASSIFICATION

Does the application access, create, receive, or process any of the following data elements? If yes, please check the box.

Social Security # □	Passport # □
Credit Card # □	Salaries □
Bank Acct. # □	Budget Info □
Employee Evaluation Info □	Veterans Administration Data □

Please provide a brief description of the data:

WITNESS

Are there witnesses to the incident? Select.   If yes, please provide name(s):

Address:

Phone No.:

Reporting Persons Signature □ Date □

CIO/IT Manager Signature □ Date □

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.