Cybersecurity Policy Handbook for Trust Tech

# **Acceptable Use Policy**

## Acceptable Use:

Personnel are responsible for complying with Trust Tech policies when using company information resources and/or on company time. If requirements or responsibilities are unclear, please seek assistance from the Information Security Committee.

This Acceptable Use Policy (AUP) governs the appropriate use of computer systems and networks owned or operated by Trust Tech. All users of these systems and networks are required to adhere to this policy to ensure the security, integrity, and proper functioning of the organization's resources.

## Unauthorized Access

Users are strictly prohibited from accessing any computer system or network without proper authorization. This includes any attempt to gain unauthorized access to systems or networks owned or operated by Trust Tech, as well as any unauthorized attempts to access systems or networks belonging to external entities.

## Unauthorized Access to Data

Users must not attempt to access any data for which they do not have explicit authorization. This includes but is not limited to data that is confidential, proprietary, or protected by law. Users must respect the confidentiality and privacy of data and only access information necessary for their job responsibilities.

## Keeping Equipment Safe

Users are responsible for the safety and security of the equipment assigned to them. This includes protecting equipment from physical damage, theft, and unauthorized access. Users must employ appropriate security measures, such as password protection and encryption, to safeguard their equipment and prevent unauthorized use.

## Prohibited Activities

The following activities are strictly prohibited and must not be engaged in while using company computer systems and networks:

### 1. Pornography:

Users must not access, download, distribute, or display any sexually explicit or pornographic material. This includes explicit content of any nature that may be offensive, inappropriate, or in violation of applicable laws and regulations.

### 2. Military Related:

Users must not engage in any activities that are related to military operations, national security, or any activities that may compromise the security and interests of the organization or its stakeholders.

### 3. Gambling:

Users must not participate in any form of online gambling or engage in any activities that involve placing bets or wagers using company resources. This includes accessing online casinos, sports betting platforms, or any other gambling-related websites.

### 4. Online Shopping:

Users must refrain from engaging in personal online shopping activities using company resources. This includes making purchases, browsing e-commerce websites, or conducting any commercial transactions unrelated to company operations.

Violation of this AUP may result in disciplinary action, including but not limited to termination of employment or legal action. If users have any questions or need clarification regarding the acceptable use of computer systems and networks, they should contact their supervisor or the IT department.

By adhering to this AUP, users contribute to maintaining a secure and productive computing environment that benefits the organization and its stakeholders.

## Mapped Controls:

This AUP aligns with relevant sections and sub-categories of the Cybersecurity Framework (CSF) and NIST Controls, emphasizing the following:

CSF Section: Asset Management

Sub-Category: 4.1 - Asset Management: This AUP mandates users to keep their assigned equipment safe from harm and prevent unauthorized access, aligning with asset management best practices.

CSF Section: Access Control

Sub-Category: 4.2 - Access Control: This AUP prohibits unauthorized access to computer systems and data, emphasizing the importance of proper access controls and authorization processes.

CSF Section: Security Awareness and Training

Sub-Category: 4.3 - Awareness and Training: This AUP requires users to be aware of the acceptable use of computer systems and networks, as well as the prohibited activities listed. It emphasizes the need for ongoing security awareness and training.

- NIST Control AC-1: Access Control Policy

- NIST Control AC-2: Account Management

- NIST Control AC-3: Access Enforcement

- NIST Control AC-4: Information Flow Enforcement

- NIST Control AC-5: Separation of Duties

- NIST Control AC-6: Least Privilege

- NIST Control AC-7: Unsuccessful Logon Attempts

## RACI Matrix

In a RACI matrix, tasks or activities are listed along the rows, and team members or stakeholders are listed along the columns. Each cell in the matrix is assigned a role designation:

**Responsible (R):** The person or team responsible for completing the task or activity. They are directly involved in its execution.

**Accountable (A):** The person who ultimately owns the task and is answerable for its success. They ensure that the task is completed and may delegate responsibilities to others.

**Consulted (C):** The individuals who provide input or expertise to the task. They are consulted for their insights or advice but are not directly responsible for the task's completion.

**Informed (I):** The individuals who need to be kept informed about the task's progress or outcomes. They are updated on the task's status but are not directly involved in its execution.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task/Responsibility** | **Responsible** | **Accountable** | **Consulted** | **Informed** |
| Policy Development | IT Security Officer | IT Manager | Legal Counsel, HR Manager | Compliance Officer, Senior Management |
| Policy Review and Approval | IT Manager | Compliance Officer | Legal Counsel, IT Security Officer | HR Manager, Senior Management |
| Policy Communication and Training | HR Manager | IT Manager | IT Security Officer, Compliance Officer | All Employees |
| Monitoring and Enforcement | IT Security Officer | IT Manager | HR Manager, Legal Counsel | Compliance Officer, Senior Management |
| Incident Reporting and Handling | All Employees | IT Security Officer | IT Manager, HR Manager | Compliance Officer, Legal Counsel |
| Periodic Policy Review and Update | IT Manager | IT Security Officer | Compliance Officer, Legal Counsel | Senior Management, HR Manager |

## Version Control Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 0.1 | 02-06-2023 | Initial Draft created | Ubaid Thoufiq |
| 0.1.1 | 03-06-2023 | Suggested changes to Citations format and misspelt words | 700746556, 700754043 |
| 0.1.2 | 03-06-2023 | Made changes to Document following the suggestions made by peer review team. | Ubaid Thoufiq |
| 0.1.3 | 03-06-2023 | Peer Reviewed | 700746556, 700754043 |
| 1.0 | 03-06-2023 | Submitted the copy for review | Ubaid Thoufiq |
| 1.1 | 10-06-2023 | Added RACI matrix and Version Control Table | Ubaid Thoufiq |

# **Asset Management Policy**

## Asset Management:

This Asset Management Policy establishes guidelines and procedures for the effective management of assets, with a focus on backups. It aims to ensure the availability, integrity, and confidentiality of organizational data and systems through regular and reliable backup processes.

## Scope:

This policy applies to all employees, contractors, and third-party vendors who have access to organizational assets and are responsible for conducting backups.

## Policy Guidelines:

### 1. Backups:

The primary focus of this policy is on backups. All assets, including critical data, system configurations, and other important information, must be regularly backed up to mitigate the risk of data loss or system failures.

### 2. Backup Frequency:

Regular backups must be performed as per defined schedules, taking into consideration the criticality of data and systems. The frequency of backups should align with the recovery objectives defined by the organization.

### 3. Backup Integrity:

Backups must be conducted in a manner that ensures the integrity of the data. This includes verifying the completeness and accuracy of backups through validation processes and periodic testing of the restore procedures.

### 4. Storage and Retention:

Backed-up data should be stored in secure locations, such as off-site or cloud-based backup systems, to protect against physical damage or loss. Retention periods for backups should be defined based on business requirements, compliance obligations, and legal considerations.

### 5. Access Controls:

Access to backup systems and media should be restricted to authorized personnel only. Access control mechanisms, including strong authentication and least privilege principles, must be implemented to prevent unauthorized access or tampering.

Personnel are responsible for complying with Trust Tech policies when using company information resources and/or on company time. If requirements or responsibilities are unclear, please seek assistance from the Information Security Committee.

## Mapped controls: CSF Section: ID.AM - Identify (Asset Management); CSF Sub-Category: Asset Management. Below are the Related NIST 800-53v5 Controls:

- NIST-V5

- NIST Control AC-2 Account Management

- NIST Control AU-6: Audit Review, Analysis, and Reporting

- NIST Control CP-2: Contingency Planning Policy and Procedures

- NIST Control RA-5: Vulnerability Scanning

- NIST Control PE-3: Physical Access Control

- NIST Control MP-3: Media Access

## RACI Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task/Responsibility** | **Responsible** | **Accountable** | **Consulted** | **Informed** |
| Policy Development | IT Security Officer | IT Manager | Compliance Officer, Legal Counsel | Senior Management, Asset Owners |
| Policy Review and Approval | IT Manager | Compliance Officer | Legal Counsel, IT Security Officer | Senior Management, Asset Owners |
| Policy Communication and Training | HR Manager | IT Manager | IT Security Officer, Compliance Officer | All Employees, Asset Owners |
| Asset Inventory Maintenance | IT Asset Manager | IT Security Officer | IT Manager, Compliance Officer | Asset Owners, IT Support Staff |
| Asset Classification and Tagging | IT Asset Manager | IT Security Officer | Compliance Officer, Legal Counsel | Asset Owners, IT Support Staff |
| Asset Tracking and Monitoring | IT Asset Manager | IT Security Officer | IT Manager, Compliance Officer | Asset Owners, IT Support Staff |
| Risk Assessment and Mitigation | IT Security Officer | IT Manager | Compliance Officer, Legal Counsel | Asset Owners, Risk Management Team |
| Disposal and Decommissioning | IT Asset Manager | IT Security Officer | Compliance Officer, Legal Counsel | Asset Owners, IT Support Staff |
| Periodic Asset Audit and Verification | IT Asset Manager | IT Security Officer | Compliance Officer, Internal Audit | Senior Management, Asset Owners |

## Version Control Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 0.1 | 02-06-2023 | Initial Draft created | Ubaid Thoufiq |
| 0.1.3 | 03-06-2023 | Peer Reviewed | 700746556, 700754043 |
| 1.0 | 03-06-2023 | Submitted the copy for review | Ubaid Thoufiq |
| 1.1 | 10-06-2023 | Added RACI matrix and Version Control Table | Ubaid Thoufiq |

# Logging Standard

This Logging Standard establishes guidelines and procedures for the effective logging practices within Trust Tech. It defines how logging will be implemented, what will be logged, and aligns with relevant Cybersecurity Framework (CSF) and NIST Controls to ensure the integrity, availability, and confidentiality of log data.

## Scope

This standard applies to all systems and applications owned or operated by Trust Tech that generate log data.

## Standard Guidelines

### 1. Logging Implementation:

a. All systems and applications must implement logging mechanisms to capture relevant security events and activities.

b. Logging should be performed at appropriate levels of granularity, including network, system, and application layers.

### 2. Logging Content:

a. The standard requires the logging of specific security-related events, including but not limited to authentication attempts, access control changes, system and application errors, and suspicious activities.

b. Log entries should contain relevant details such as timestamps, source and destination IP addresses, usernames, and event descriptions.

### 3. Log Storage and Retention:

a. Log data should be securely stored on centralized and protected log servers or systems to prevent unauthorized access or tampering.

b. Retention periods for logs should be defined based on legal, regulatory, and business requirements, ensuring that logs are retained for an appropriate duration.

## Mapped Controls

This Logging Standard aligns with relevant sections and sub-categories of the Cybersecurity Framework (CSF) and NIST Controls, emphasizing the following:

CSF Section: Detection Processes

- Sub-Category: 4.2 - Event detection: This standard contributes to the detection process by defining logging practices to capture security events effectively.

CSF Section: Response Planning

- Sub-Category: 5.1 - Response plan: This standard enables effective response planning by ensuring the availability of detailed logs to aid in incident investigation and analysis.

NIST 800-53v5 Controls used by Trust Tech include:

- NIST Control AU-2: Auditable Events

- NIST Control AU-3: Content of Audit Records

- NIST Control AU-6: Audit Review, Analysis, and Reporting

- NIST Control AU-7: Audit Reduction and Report Generation

- NIST Control AU-8: Time Stamps

- NIST Control AU-9: Protection of Audit Information

- NIST Control SI-4: Information System Monitoring

- NIST Control SI-7: Software, Firmware, and Information Integrity

Employees and system administrators are required to adhere to this Logging Standard. Non-compliance may result in disciplinary action, including but not limited to loss of privileges, retraining, or termination, as determined by the severity and frequency of the violation.

## RACI Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task/Responsibility** | **Responsible** | **Accountable** | **Consulted** | **Informed** |
| Policy Development | IT Security Officer | IT Manager | Compliance Officer, Legal Counsel | Senior Management, System Administrators |
| Policy Review and Approval | IT Manager | Compliance Officer | Legal Counsel, IT Security Officer | Senior Management, System Administrators |
| Policy Communication and Training | HR Manager | IT Manager | IT Security Officer, Compliance Officer | All Employees, System Administrators |
| Logging Implementation | System Administrators | IT Security Officer | IT Manager, Compliance Officer | IT Operations Team, IT Support Staff |
| Defining Log Content | IT Security Officer | IT Manager | Compliance Officer, Legal Counsel | System Administrators, IT Support Staff |
| Log Storage and Retention | IT Security Officer | IT Manager | Compliance Officer, Data Privacy Officer | System Administrators, IT Operations Team |
| Monitoring and Alerting | IT Security Officer | IT Manager | Compliance Officer, SOC Team | System Administrators, IT Operations Team |
| Log Analysis and Reporting | IT Security Officer | IT Manager | Compliance Officer, SOC Team | Senior Management, Data Privacy Officer |
| Incident Response and Investigation | IT Security Officer | IT Manager | Compliance Officer, Legal Counsel | System Administrators, Incident Response Team |

## Version Control Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 0.1 | 02-06-2023 | Initial Draft created | Ubaid Thoufiq |
| 0.1.3 | 03-06-2023 | Peer Reviewed | 700746556, 700754043 |
| 1.0 | 03-06-2023 | Submitted the copy for review | Ubaid Thoufiq |
| 1.1 | 10-06-2023 | Added RACI matrix and Version Control Table | Ubaid Thoufiq |

# Information Disposal Standard

This Information Disposal Standard establishes guidelines and procedures for the secure and proper disposal of sensitive information within Trust Tech. It defines what will be disposed of, how it will be disposed of, and follows the relevant National Institute of Standards and Technology (NIST) Special Publication 800-88 Rev. 1 guidelines for media sanitization. This standard also incorporates audit trail mechanisms to ensure proper tracking and accountability during the disposal process.

## Scope

This standard applies to all employees, contractors, and third-party vendors who handle or have access to sensitive information that requires disposal.

## Standard Guidelines

### 1. Disposal Content:

a. This standard applies to all types of sensitive information, including but not limited to physical documents, electronic files, storage media, and obsolete hardware.

b. Information that is no longer needed or has reached its retention period, and poses a risk if improperly disclosed, should be identified for disposal.

### 2. Disposal Methods:

a. Disposal methods should be appropriate to the type of information being disposed of, considering factors such as sensitivity and confidentiality.

b. Paper documents should be shredded using cross-cut or micro-cut shredders to render them irrecoverable.

c. Electronic media, including hard drives and portable storage devices, should be securely erased or physically destroyed according to NIST SP 800-88 Rev. 1 guidelines.

### 3. NIST 800-88 Rev. 1 Guidelines:

a. Trust Tech follows the media sanitization guidelines outlined in NIST Special Publication 800-88 Rev. 1 for secure disposal of electronic media and storage devices.

b. Media sanitization methods, including clearing, purging, and destruction, should be selected based on the sensitivity of the information and the type of media.

### 4. Audit Trail:

a. An audit trail must be maintained to track the disposal process, including documentation of the disposed items, disposal methods used, and responsible personnel.

b. The audit trail should include information such as disposal dates, disposal locations, and any relevant approvals or authorizations.

## Mapped Controls:

This Information Disposal Standard aligns with relevant sections and sub-categories of the Cybersecurity Framework (CSF) and NIST Controls, emphasizing the following:

CSF Section: Protect

- Sub-Category: 3.6 - Data disposal: This standard ensures the secure disposal of sensitive information, aligning with data protection objectives.

NIST 800-53v5 Controls used by Trust Tech

- NIST Control MP-6: Media Sanitization and Disposal

- NIST Control AU-8: Time Stamps

- NIST Control SI-4: Information System Monitoring

- NIST Control AC-2: Account Management

- NIST Control AC-6: Least Privilege

- NIST Control AC-19: Access Control for Portable and Mobile Devices

## RACI Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task/Responsibility** | **Responsible** | **Accountable** | **Consulted** | **Informed** |
| Policy Development | IT Security Officer | IT Manager | Compliance Officer, Legal Counsel | Senior Management, System Administrators |
| Policy Review and Approval | IT Manager | Compliance Officer | Legal Counsel, IT Security Officer | Senior Management, System Administrators |
| Policy Communication and Training | HR Manager | IT Manager | IT Security Officer, Compliance Officer | All Employees, System Administrators |
| Logging Implementation | System Administrators | IT Security Officer | IT Manager, Compliance Officer | IT Operations Team, IT Support Staff |
| Defining Log Content | IT Security Officer | IT Manager | Compliance Officer, Legal Counsel | System Administrators, IT Support Staff |
| Log Storage and Retention | IT Security Officer | IT Manager | Compliance Officer, Data Privacy Officer | System Administrators, IT Operations Team |
| Monitoring and Alerting | IT Security Officer | IT Manager | Compliance Officer, SOC Team | System Administrators, IT Operations Team |
| Log Analysis and Reporting | IT Security Officer | IT Manager | Compliance Officer, SOC Team | Senior Management, Data Privacy Officer |
| Incident Response and Investigation | IT Security Officer | IT Manager | Compliance Officer, Legal Counsel | System Administrators, Incident Response Team |

## Version Control Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 0.1 | 02-06-2023 | Initial Draft created | Ubaid Thoufiq |
| 0.1.3 | 03-06-2023 | Peer Reviewed | 700746556, 700754043 |
| 1.0 | 03-06-2023 | Submitted the copy for review | Ubaid Thoufiq |
| 1.1 | 10-06-2023 | Added RACI matrix and Version Control Table | Ubaid Thoufiq |

# Logging Procedure

## Procedure:

Enabling and Forwarding Logging to Trust Tech -SIEM

## Objective:

The objective of this procedure is to enable and configure logging on a selected server and forward the logs to the Trust Tech Security and Incident Event Manager (SIEM) with the following details:

- SIEM Name: Trust Tech -SIEM

- Private IP Address: 10.10.10.250

## Prerequisites:

- Access to the server with administrative privileges.

- The Logging Standard for Trust Tech (reference Logging Standard by Ubaid Thoufiq).

## Steps:

### 1. Introduction:

This procedure outlines the steps to enable and configure logging on the selected server and forward the logs to the Trust Tech -SIEM for centralized monitoring and analysis. It aligns with the Logging Standard by Ubaid Thoufiq for Trust Tech.

### 2. Logging Configuration:

a. Log in to the selected server using administrative credentials.

b. Open the server's logging configuration file (e.g., /etc/rsyslog.conf or /etc/syslog-ng/syslog-ng.conf) using a text editor.

### 3. Enable Logging:

a. Locate the logging configuration section in the file.

b. Uncomment or add the necessary configuration lines to enable logging, such as:

- For rsyslog:

```

\*.\* @10.10.10.250

```

- For syslog-ng:

```

destination logserver { tcp("10.10.10.250"); };

log { source(s\_src); destination(logserver); };

```

### 4. Save and Close the Configuration File:

Save the changes made to the logging configuration file and close the text editor.

### 5. Restart Logging Service:

a. Depending on the server's operating system, restart the logging service to apply the changes. Use the appropriate command, such as:

- For rsyslog: `sudo systemctl restart rsyslog`

- For syslog-ng: `sudo systemctl restart syslog-ng`

### 6. Verify Logging:

a. Monitor the server's logs to ensure that logging events are being generated.

b. Tail or view the logs in real-time using commands like `tail -f /var/log/syslog` or `journalctl -f`.

### 7. Log Forwarding to Trust Tech -SIEM:

a. Access the Trust Tech -SIEM management console.

b. Configure a new log source with the following details:

- Log Source Name: [Server Name]

- Log Source IP Address: [Server IP Address]

- Log Source Type: [Server Operating System]

- Log Forwarding Protocol: TCP or UDP (based on your environment)

- Log Forwarding Destination: 10.10.10.250

### 8. Test and Validation:

a. Verify that logs from the server are being received by the Trust Tech -SIEM.

b. Review the log data in the SIEM console to ensure the logs are accurately forwarded.

## Conclusion:

Logging on the selected server has been enabled and configured to forward logs to the Trust Tech -SIEM. This ensures centralized monitoring and analysis of log data for enhanced security and incident response capabilities.

## Mapped Controls:

CSF Section: Protect: 3.6 - Data Disposal, 4.2 - Event Detection

NIST Control: AU-4 - Audit Storage Capacity, AC-6 - Least Privilege

## RACI matrix for Logging Procedure:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task/Activity** | **Responsible** | **Accountable** | **Consulted** | **Informed** |
| Define logging requirements | Security Analyst | IT Manager | Compliance | CISO |
| Develop Logging Procedure | Security Analyst | IT Manager | Compliance | CISO |
| Implement logging mechanism | Security Analyst | IT Manager | Compliance | CISO |
| Test logging functionality | IT Manager | IT Manager | Compliance | CISO |
| Review and update logging procedure | Compliance | IT Manager | IT Manager, CISO | CISO |

## Version Control Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 0.1 | 08-06-2023 | Initial Draft created | Ubaid Thoufiq |
| 0.1.3 | 03-06-2023 | Peer Reviewed | 700746556, 700754043 |
| 1.0 | 09-06-2023 | Submitted the copy for review | Ubaid Thoufiq |
| 1.1 | 10-06-2023 | Added RACI matrix and Version Control Table | Ubaid Thoufiq |

# Information Disposal Procedure

## Procedure:

* 1. Information Disposal Procedure for Trust Tech

## Objective:

* 1. The objective of this procedure is to establish guidelines and instructions for the proper disposal of physical documents, electronic media, storage media, and obsolete hardware in accordance with the Information Disposal Standard of Trust Tech. By following this procedure, we aim to ensure the secure and compliant disposal of sensitive information, mitigate the risk of data breaches, and comply with legal, regulatory, and business requirements.

## Prerequisites:

* 1. 1. Familiarity with the Information Disposal Standard of Trust Tech.  
     2. Access to approved data destruction tools or contract with reputable data destruction service providers.  
     3. Knowledge of NIST 800-88 Rev. 1 guidelines for selecting appropriate sanitization methods.  
     4. Awareness of the company's document retention policy and hardware disposal regulations.

## Steps:

1. **Disposal of Physical Documents, Electronic Media, Storage Media, and Obsolete Hardware:**  
 a. **Physical Documents:**  
 i. Shred all sensitive and confidential physical documents using a cross-cut shredder or contract with a certified document destruction service.  
 ii. Ensure that all shredded documents are securely collected and disposed of in designated waste bins.  
 iii. Follow the company's document retention policy to determine which documents can be safely disposed of.  
  
 b. **Electronic Media and Storage Media:**  
 i. Identify all electronic media and storage devices that need to be disposed of, including hard drives, solid-state drives (SSDs), USB drives, CDs/DVDs, and magnetic tapes.  
 ii. For hard drives and SSDs, use a secure sanitation method to prevent data recovery. Follow the NIST 800-88 Rev. 1 guidelines for proper sanitization procedures.  
 iii. Use data destruction tools or contract with a reputable data destruction service to securely erase data from electronic media.  
 iv. For physically damaged or non-functional media, ensure their destruction through physical destruction methods, such as shredding or incineration.  
  
 c. **Obsolete Hardware:**  
 i. Identify hardware that is no longer in use or has become obsolete.  
 ii. Ensure all data is securely wiped from the hardware following the approved data destruction methods mentioned above.  
 iii. Dispose of the hardware following appropriate environmental regulations and guidelines.  
  
2. **Disposal Methods under NIST 800-88 Rev. 1 Guidelines:**  
 a. Follow the NIST 800-88 Rev. 1 guidelines for selecting appropriate sanitization methods based on the type of media and the level of sensitivity of the data stored.  
 b. Use methods such as Secure Erase, Cryptographic Erase, Degaussing, Physical Destruction, or Sanitization through overwriting to ensure data cannot be recovered.  
  
3. **Audit Trail for Information Disposal Process:**  
 a. Maintain an audit trail to track the entire information disposal process.  
 b. Document the details of disposed physical documents, electronic media, storage media, and obsolete hardware, including dates, responsible personnel, and disposal methods used.  
 c. Ensure the audit trail is securely stored and retained for the required period as per legal, regulatory, and business requirements.  
  
Note: Please refer to the "Information Disposal Standard" for Trust Tech for detailed instructions and specific guidelines related to the information disposal process.

## Conclusion:

The information disposal procedure outlined in this document provides clear instructions for the proper disposal of physical documents, electronic media, storage media, and obsolete hardware. By following this procedure, Trust Tech ensures the secure erasure of sensitive data and the compliant disposal of information assets. Adhering to the Information Disposal Standard and leveraging the guidelines provided by NIST 800-88 Rev. 1, we maintain the integrity, confidentiality, and availability of information, reduce the risk of unauthorized access or data breaches, and demonstrate our commitment to information security and regulatory compliance.

## Mapped Controls:

NIST controls: PE-20 - Securely Dispose of Information System Components, AU-1 - Audit and Accountability Policy and Procedures, MP-6 - Media Sanitization and Disposal, AC-19 - Access Control for Portable and Mobile Devices

## RACI matrix for Information Disposal Procedure:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task/Activity** | **Responsible** | **Accountable** | **Consulted** | **Informed** |
| Identify documents and media for disposal| | IT Manager | IT Manager | Compliance, Legal | CISO |
| Determine appropriate disposal methods | IT Manager | IT Manager | Compliance | CISO |
| Shredding of physical documents | Facilities Staff | IT Manager | Compliance | CISO |
| Secure erasure of electronic media | IT Staff | IT Manager | Compliance, Legal | CISO |
| Destruction of obsolete hardware | Facilities Staff | IT Manager | IT Manager, CISO | CISO |
| Maintaining audit trail | IT Manager | Compliance | Legal | CISO |

## Version Control Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 0.1 | 08-06-2023 | Initial Draft created | Ubaid Thoufiq |
| 0.1.3 | 03-06-2023 | Peer Reviewed | 700746556, 700754043 |
| 1.0 | 09-06-2023 | Submitted the copy for review | Ubaid Thoufiq |
| 1.1 | 10-06-2023 | Added RACI matrix and Version Control Table | Ubaid Thoufiq |

# BYOD GUIDELINES

## Guidelines:

* 1. Bring Your Own Device (BYOD) Guidelines for Trust Tech

## Introduction:

* 1. Bring Your Own Device (BYOD) refers to the practice of employees using their personal devices, such as smartphones, laptops, or tablets, for work-related activities. This guideline aims to provide guidance on the adoption of BYOD within our organization and whether it should be permitted or not. While there is no definitive right or wrong answer, it is crucial to consider various factors and make an informed decision based on the organization's specific needs and security requirements.

## Considerations for Permitting BYOD:

### 1. Employee Productivity and Satisfaction:

* 1. - BYOD can enhance employee productivity by allowing them to work on devices they are familiar with and prefer to use.  
      - Employees may experience increased job satisfaction and flexibility by using their own devices, leading to higher motivation and engagement.

### 2. Cost Savings:

* 1. - Permitting BYOD can reduce the organization's expenditure on purchasing and maintaining company-owned devices.  
      - Employees bear the cost of acquiring and maintaining their devices, potentially resulting in cost savings for the organization.

### 3. Enhanced Collaboration and Communication:

* 1. - BYOD can facilitate seamless communication and collaboration between employees, as they can access work-related information and tools anytime, anywhere.  
      - Integration of personal devices with work applications and platforms may lead to improved teamwork and responsiveness.

### 4. Increased Employee Responsibility:

* 1. - Employees using their personal devices for work may have a heightened sense of responsibility and care for their devices, leading to better device security practices.

## Security and Privacy Concerns:

### 1. Data Security:

* 1. - BYOD introduces risks related to the loss, theft, or unauthorized access to sensitive company data. Proper security measures must be implemented to mitigate these risks.  
      - Encryption, strong authentication mechanisms, and secure data storage should be mandatory for all BYOD devices.

### 2. Device Management:

* 1. - Implement a Mobile Device Management (MDM) solution to enforce security policies, such as remote wipe, device encryption, and malware detection, on BYOD devices.  
      - Regular patching and software updates must be enforced to ensure devices remain secure and protected against vulnerabilities.

### 3. Privacy and Legal Considerations:

* 1. - Develop a clear BYOD policy that outlines employees' responsibilities regarding the privacy of personal data stored on their devices.  
      - Comply with relevant privacy regulations and ensure proper separation of personal and company data on BYOD devices.

## Conclusion:

* 1. The decision to permit or restrict BYOD should be based on a careful evaluation of the organization's needs, security considerations, and potential benefits. A well-defined BYOD policy, supported by strong security measures and clear guidelines, can enable the organization to harness the advantages of BYOD while effectively mitigating associated risks.

## Mapped Controls:

NIST Controls: AC-2 - Account Management, SC-13 - Cryptographic Protection, AC-3 - Access Enforcement, SI-2 - Flaw Remediation, PS-3 - Personnel Screening

## RACI matrix:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task/Activity** | **Responsible** | **Accountable** | **Consulted** | **Informed** |
| 1. Assessing organization's BYOD needs and goals | IT Manager | CIO | Legal | HR |
| 2. Developing BYOD policy and guidelines | IT Manager | Legal | HR | Employees |
| 3. Defining security requirements and measures | IT Manager | CIO | Legal | HR |
| 4. Communicating BYOD policy to employees | HR | IT Manager | Legal | Employees |
| 5. Implementing Mobile Device Management (MDM) solution and security controls | IT Manager | IT Team | CISO | HR |
| 6. Providing employee training and awareness on BYOD security practices | HR | IT Manager | Legal | Employees |
| 7. Monitoring and enforcing BYOD policy compliance | IT Manager | HR | Legal | CISO |

## Version Control Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 0.1 | 08-06-2023 | Initial Draft created | Ubaid Thoufiq |
| 0.1.3 | 03-06-2023 | Peer Reviewed | 700746556, 700754043 |
| 1.0 | 09-06-2023 | Submitted the copy for review | Ubaid Thoufiq |
| 1.1 | 10-06-2023 | Added RACI matrix and Version Control Table | Ubaid Thoufiq |

# Guidelines on Using ChatGPT in Trust Tech

## Guidelines:

* 1. Company’s Guidelines on using ChatGPT for Trust Tech

## Introduction:

* 1. ChatGPT is an advanced language model developed by OpenAI that uses artificial intelligence to generate human-like text responses. This guideline aims to provide guidance on the use of ChatGPT within Trust Tech and whether its adoption is recommended or not. While there is no definitive right or wrong answer, it is important to consider various factors and make an informed decision based on the organization's specific needs, ethical considerations, and potential benefits.

## Considerations for Using ChatGPT:

### 1. Enhanced Customer Support:

* 1. - ChatGPT can be utilized to provide instant and personalized responses to customer queries, improving customer satisfaction and response times.  
      - It can assist in handling routine inquiries, freeing up human agents' time for more complex or critical tasks.

### 2. Workflow Automation:

* 1. - ChatGPT can be integrated into various systems and processes to automate repetitive tasks, such as generating reports, drafting emails, or conducting data analysis.  
      - This can lead to increased operational efficiency and productivity by reducing manual efforts.

### 3. Language Translation and Localization:

* 1. - ChatGPT can assist in language translation and localization, allowing Trust Tech to communicate effectively with a global audience and potentially expand into new markets.  
      - It can help bridge language barriers and enable seamless multilingual interactions.

### 4. Content Generation and Personalization:

* 1. - ChatGPT can aid in generating creative content, such as blog posts, marketing materials, or product descriptions, based on given prompts or specifications.  
      - It can also enable personalized recommendations and suggestions for customers, enhancing the overall user experience.

### 5. Threat Intelligence Analysis:

* 1. - ChatGPT can assist in analyzing and understanding complex cybersecurity threats by processing vast amounts of security-related data and generating actionable insights.  
      - It can help identify patterns, detect anomalies, and provide timely threat intelligence to enhance proactive defense measures.

### 6. Incident Response and Investigation:

* 1. - ChatGPT can aid in incident response and investigation processes by quickly providing relevant information and guidance to cybersecurity teams.  
      - It can assist in analyzing log files, identifying potential indicators of compromise, and suggesting remediation steps, thereby improving incident handling efficiency.

## Ethical Considerations:

### 1. Bias and Fairness:

* 1. - Ensure that the training data used for ChatGPT is diverse, representative, and free from biases that could result in discriminatory or unethical responses.  
      - Regularly monitor and evaluate the model's outputs to mitigate any unintended biases or unfairness.

### 2. Data Privacy and Security:

* 1. - Take necessary measures to protect customer data and ensure compliance with relevant privacy regulations.  
      - Minimize the collection and storage of personal information, and implement appropriate security protocols to safeguard sensitive data.

### 3. Transparency and Explainability:

* 1. - Be transparent about the use of ChatGPT to customers and stakeholders, clearly indicating when they are interacting with an AI system.  
      - Provide explanations or disclaimers when appropriate, especially if the responses generated by ChatGPT might not be fully accurate or reliable.
  2. Guideline for "Company's" Use of ChatGPT in the Cybersecurity Industry

## Conclusion:

* 1. The decision to use ChatGPT within "Company" should consider the potential benefits it offers, such as improved customer support, workflow automation, and language translation. However, ethical considerations related to bias, privacy, and transparency must be carefully addressed. A thorough evaluation of the organization's specific needs and ethical framework should guide the decision-making process.

## Mapped Controls:

NIST controls: PR.IP-3 - Data Security, PR.IP-1 - Baseline Configuration, AU-8 - Time Stamps, AC-4 - Information Flow Enforcement, PR.AC-1 - Identities and Credentials

## RACI matrix:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task/Activity** | **Responsible** | **Accountable** | **Consulted** | **Informed** |
| 1. Develop ChatGPT guidelines | SME | Security Manager | Legal Counsel | All Employees |
| 2. Evaluate ethical considerations | SME | Legal Counsel, Compliance Officer | Security Manager, IT Manager | All Employees |
| 3. Assess cybersecurity needs | IT Manager | Security Manager | SME, Legal Counsel | All Employees |
| 4. Integrate ChatGPT into systems | IT Manager | Security Manager, SME | Compliance Officer, Legal Counsel | All Employees |
| 5. Train employees on ChatGPT usage | Security Manager | IT Manager | SME, Legal Counsel, Compliance Officer | All Employees |
| 6. Ensure data privacy and security | Compliance Officer | Legal Counsel, IT Manager | Security Manager, SME | All Employees |
| 7. Evaluate ChatGPT's effectiveness | SME | Security Manager, IT Manager | Legal Counsel, Compliance Officer | All Employees |

## Version Control Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 0.1 | 08-06-2023 | Initial Draft created | Ubaid Thoufiq |
| 0.1.3 | 03-06-2023 | Peer Reviewed | 700746556, 700754043 |
| 1.0 | 09-06-2023 | Submitted the copy for review | Ubaid Thoufiq |
| 1.1 | 10-06-2023 | Added RACI matrix and Version Control Table | Ubaid Thoufiq |

# Incident Response Plan for Lost/Stolen for Trust Tech

## Guidelines:

* 1. Incident Response Plan for Lost/Stolen Laptop with ePHI

## Introduction:

* 1. The objective of this incident response plan is to effectively respond to the loss or theft of a laptop containing electronic Protected Health Information (ePHI). The plan aims to mitigate potential risks, ensure compliance with relevant regulations, and minimize the impact on data confidentiality and integrity.

## Incident Identification and Reporting:

* 1. a. Immediately report the incident to the designated incident response team or security personnel.
  2. b. Gather specific details about the incident, including the date, time, location, and circumstances of the loss or theft.
  3. c. Determine if the laptop contains ePHI and assess the potential risk to the affected individuals.

## Laptop Encryption and Security:

* 1. a. Determine if the lost or stolen laptop is encrypted. If encrypted, document the encryption method and key management process.
  2. b. If the laptop is not encrypted, follow the organization's procedures for notifying affected individuals and regulatory bodies, as required by applicable laws and regulations.
  3. c. Activate remote wipe capabilities if available and feasible to protect the ePHI from unauthorized access.

## Incident Response Actions:

* 1. a. Secure the area where the incident occurred and limit access to authorized personnel.
  2. b. File a police report in case of theft and obtain a copy for documentation purposes.
  3. c. Initiate an investigation to gather additional information about the incident, such as potential suspects or witnesses.
  4. d. Collaborate with legal counsel and regulatory compliance officers to determine the necessary notifications and reporting to regulatory bodies and affected individuals.

## Communication and Notification:

* 1. a. Notify the appropriate internal stakeholders, including senior management, legal counsel, IT department, and human resources.
  2. b. Comply with notification requirements under applicable regulations, such as HIPAA, by notifying affected individuals within the specified timeframe.
  3. c. Provide clear and concise instructions to affected individuals on steps they should take to protect themselves from potential harm resulting from the incident.

## Recovery and Preventive Measures:

* 1. a. Evaluate the incident's impact and implement measures to prevent similar incidents in the future.
  2. b. Conduct a thorough review of existing security controls and policies related to laptop usage, encryption, physical security, and ePHI handling.
  3. c. Enhance staff training and awareness programs to reinforce proper laptop handling, data encryption, and incident reporting procedures.

## RACI matrix:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task/Responsibility** | **Responsible** | **Accountable** | **Consulted** | **Informed** |
| **Incident Identification and Reporting** | Incident Response Team | Incident Response Team Lead | Legal Counsel, Security Manager | All Employees |
| **Assess Laptop Encryption and Security** | IT Security Officer | Compliance Officer | Legal Counsel, IT Manager | Incident Response Team Lead, Security Manager |
| **Activate Remote Wipe** | IT Security Officer | IT Manager | Legal Counsel, Incident Response Team Lead | Compliance Officer, Security Manager |
| **Secure Incident Area** | Security Personnel | IT Manager | Incident Response Team Lead | All Employees |
| **File Police Report** | Security Personnel | Legal Counsel | Incident Response Team Lead | All Employees |
| **Initiate Investigation** | Security Personnel | Incident Response Team Lead | Legal Counsel, Compliance Officer | All Employees |
| **Communicate with Internal Stakeholders** | Incident Response Team Lead | Senior Management | Legal Counsel, IT Manager, HR Manager | All Employees |
| **Comply with Regulatory Notifications** | Compliance Officer | Legal Counsel | Incident Response Team Lead, IT Manager | All Employees |
| **Notify Affected Individuals** | Incident Response Team Lead | Compliance Officer | Legal Counsel, IT Manager | All Employees |
| **Review Security Controls and Policies** | IT Security Officer | IT Manager | Legal Counsel, Compliance Officer | Incident Response Team Lead, Security Manager |
| **Enhance Training and Awareness Programs** | Training and Development Manager | HR Manager | Compliance Officer, IT Manager | All Employees |

## Version Control Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 1 | 13-06-2023 | Initial draft of the incident response plan. | Ubaid Thoufiq |
| 1.1 | 13-06-2023 | Reviewed and incorporated feedback. | Ubaid Thoufiq |
| 0.1.3 | 13-06-2023 | Peer Reviewed | 700746556, 700754043 |
| 2 | 13-06-2023 | Updated plan with revised procedures based on incident response best practices and regulatory requirements. | Ubaid Thoufiq |

## **Citations:**

Acceptable use policy - state of Michigan. (n.d.). https://www.michigan.gov/-/media/Project/Websites/msp/cjic/pdfs7/Acceptable\_Use\_Policy.pdf?rev=92ed3b3dd19749358f6f6613f04ac254

Adam B. (2021, March 18). *What exactly should we be logging?* Www.ncsc.gov.uk. <https://www.ncsc.gov.uk/blog-post/what-exactly-should-we-be-logging>

Anna Mikhaylova. (n.d.). *How large language models are Changing Threat Intelligence Report analysis*. RSAconference. https://www.rsaconference.com/library/blog/how-large-language-models-are-changing-threat-intelligence-report-analysis

Cobb, M. (2023). *Security log management and logging best practices*. Google.com. https://www.techtarget.com/searchsecurity/tip/Security-log-management-and-logging-best-practices

Compliancy Group. (2022, October 31). *HIPAA Cyber Incident Response Requirements*. Compliancy Group. https://compliancy-group.com/hipaa-cyber-incident-response-requirements/#:~:text=HIPAA%20requires%20healthcare%20organizations%20to

CSF TOOLS. (2020, August 13). *AC: Access Control - CSF Tools*. Csf.tools. https://csf.tools/reference/nist-sp-800-53/r4/ac/

CSFtools. (2020, March 24). *Welcome to CSF Tools - CSF Tools*. Csf.tools. https://csf.tools

CSRC NIST. (2014, August 4). *NIST SP 800-12: Chapter 18 - Audit Trails*. Csrc.nist.rip. https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter18.html

Dashlane. (2023, January 10). *How Businesses with a BYOD Policy Can Secure Employee Devices*. Dashlane. https://www.dashlane.com/blog/ways-to-make-sure-employee-devices-secured

Davenport, T. H., & Mittal, N. (2022, November 14). *How Generative AI Is Changing Creative Work*. Harvard Business Review. https://hbr.org/2022/11/how-generative-ai-is-changing-creative-work

Dept of Education. (2014). *Best Practices for Data Destruction | Protecting Student Privacy*. Studentprivacy.ed.gov. https://studentprivacy.ed.gov/resources/best-practices-data-destruction

FRSecure. (2021, July 29). *Acceptable Use Policy Template | FRSecure*. Frsecure.com. https://frsecure.com/acceptable-use-policy-template/

Haythem OUESLATI. (2023). *Revolutionizing Learning Content Development: The Impact of AI Large Language Models | SAP Blogs*. Blogs.sap.com. https://blogs.sap.com/2023/02/16/revolutionizing-learning-content-development-the-impact-of-ai-language-models/

Hughes, A. (2023, May 16). *ICSE Spotlight: Large-language models for automatic cloud incident management*. Microsoft Research. https://www.microsoft.com/en-us/research/blog/large-language-models-for-automatic-cloud-incident-management/

Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014, December 17). *Guidelines for Media Sanitization*. Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

Mitrovic, Z., Veljkovic, I., Whyte, G., & Thompson, K. (2014). Introducing BYOD in an organisation: The risk and customer services viewpoints. Paper presented at the 1st Namibia Customer Service Awards & Conference, 2014. *Ir.nust.na*. https://ir.nust.na/handle/10628/522

National Cyber Security Centre. (2021, June 29). *Bring your own device (BYOD)*. Www.ncsc.gov.uk. https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device

NCCOE NIST. (n.d.). *Mobile Device Security: Bring Your Own Device | NCCoE*. Www.nccoe.nist.gov. https://www.nccoe.nist.gov/mobile-device-security/bring-your-own-device

Pazzanese, C. (2020, October 26). *Ethical concerns mount as AI takes bigger decision-making role*. Harvard Gazette; Harvard University. https://news.harvard.edu/gazette/story/2020/10/ethical-concerns-mount-as-ai-takes-bigger-decision-making-role/

Ross, R., Pillitteri, V., Guissanie, G., Wagner, R., Graubart, R., & Bodeau, D. (2021, February 2). *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*. Csrc.nist.gov. <https://csrc.nist.gov/publications/detail/sp/800-172/final>

Smith, G. (2023). *What does “fairness” mean for machine learning systems?* Https://Haas.berkeley.edu/. https://haas.berkeley.edu/equity/

Terry, I. (2020, December 18). *How Long Do We Need to Keep Data? | Data Retention Requirements*. Https://Www.ispartnersllc.com/. https://www.ispartnersllc.com/blog/standards-developing-data-retention-policy/

Uberoi, A. (2022, April 26). *NIST Incident Response Plan Steps & Template*. Www.cm-Alliance.com. https://www.cm-alliance.com/cybersecurity-blog/nist-incident-response-plan-steps-template

Uchicago. (n.d.). *Incident Response -Lost/Stolen Device*. https://bpb-us-w2.wpmucdn.com/voices.uchicago.edu/dist/3/3185/files/2021/06/BSD-LOST-STOLEN-CHEATSHEET-2018.pdf

University of Washington. (n.d.). *Destroying Records | Records Management Services*. Finance.uw.edu. https://finance.uw.edu/recmgt/managing/pastretention