Acceptable Use Policy (AUP)

Mohith Naga Adithya Vasamsetti

University of Central Missouri

700760007

Introduction:

An Acceptable Use Policy (AUP) sets forth the allowed and prohibited behaviours when utilizing computing resources in a company. It guarantees that all users follow legal and security policies, safeguarding the organization's assets and reputation. This policy focuses on preventing unauthorized entry into computers and data, proper equipment handling, and limitations on certain online activities.

Policy Elements:

- **Unauthorized Access to the Computer**
    - Users are prohibited from participating in actions that provide them with unauthorized entry to any computer systems. This involves circumventing security protocols or trying to penetrate networks or accounts through hacking.
- **Unauthorized Access to Data**
    - Access to sensitive or confidential information is tightly regulated. Users are prohibited from trying to access data without specific authorization. Violating this policy will result in disciplinary measures being taken.
- **Equipment Safety**
    - It is the user's responsibility to ensure that their equipment is protected from damage. This involves safeguarding devices when not being used, preventing physical harm, and promptly reporting any loss or theft.
- **Prohibited Online Activities**
    - Users are prohibited from accessing or exploring websites and content related to the following categories:

- Pornography
- Military-related content
- Gambling
- Online shopping

Engaging in these activities can expose the organization to security risks and legal liabilities.

Best Practices for AUP Compliance:

To ensure compliance with this AUP, the following best practices are recommended:

1. **Legal Department Involvement**: Ensure the legal department is involved in the creation and periodic review of the AUP to maintain legal compliance (Kirvan, P. (n.d.)
2. **Clear Communication**: Write the policy in clear, non-technical language to ensure all users understand the rules and expectations (Kirvan, P. (n.d.)
3. **Training and Awareness**: Conduct regular training sessions to educate employees about the AUP and its importance in protecting the organization (Scheldt, 2024).
4. **Regular Updates**: Update the AUP regularly to reflect changes in technology and the business environment (Scheldt, 2024).

Mapped Controls:

- **Unauthorized Access to the Computer**
    - CSF Section and Sub-Category: ID. GV-1
    - Related 800-53v5 Controls: AC-1 Policy and Procedures
- **Unauthorized Access to Data**
    - CSF Section and Sub-Category: PR.AC-1

- Related 800-53v5 Controls: AC-3 Access Enforcement

- **Equipment Safety**
  - CSF Section and Sub-Category: PR.DS-2
  - Related 800-53v5 Controls: CP-9 Contingency Planning
- **Prohibited Online Activities**
  - CSF Section and Sub-Category: PR.PT-1
  - Related 800-53v5 Controls: SI-4 Information System Monitoring

RACI Matrix:

Activity	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Unauthorized Access to the Computer	IT Security Team	CIO	Legal Department, HR	All Users
Unauthorized Access to Data	IT Security Team	CIO	Legal Department, HR	All Users
Equipment Safety	All Users	Department Heads	IT Support, Security Team	All Users
Prohibited Online Activities	IT Security Team	CIO	Legal Department, HR	All Users
Legal Department Involvement	Legal Department	CIO	IT Security Team, HR	All Users
Clear Communication	HR	CIO	Legal Department, IT Security Team	All Users
Training and Awareness	HR	CIO	IT Security Team, Department Heads	All Users
Regular Updates	IT Security Team	CIO	Legal Department, HR	All Users

Version Control:

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0		July 2024		Final Turn in and Approved Version
0.5	July 2024		700758100	No Changes needed
0.4	July 2024		700765919	No Changes needed
0.3	July 2024		700760007	Modified the Document
0.2	July 2024		Dr.M	APA isn't correct
0.1	July 2024		700760007	Initial Document creation

Asset Management Policy: Backup Focus

Mohith Naga Adithya Vasamsetti

University of Central Missouri

700760007

Introduction:

Efficient backup control is vital for organizational resilience, guaranteeing data availability and continuity in times of disruptions. This policy establishes guidelines and processes to protect the integrity and accessibility of backups in the organization.

Policy Elements:

- **Backup Definition and Scope:**
    - **Definition:** Backups refer to the replication of critical data to secure locations for recovery purposes (Goncalves, T., 2024).
    - **Scope:** This policy applies to all backup operations across organizational systems, including data centres and remote locations.
- **Benefits of Backup Management:**
    - **Operational Continuity**: Ensures continuous business operations by maintaining reliable backup systems (RedBeam, 2024).
    - **Disaster Recovery Preparedness:** Facilitates rapid recovery of critical data in the event of system failures or cyber incidents (Userflow, 2021).
- **Policy Purpose and Importance:**
    - **Objective**: To establish guidelines for the systematic management of backup assets, ensuring their availability, integrity, and confidentiality throughout their lifecycle.
    - **Alignment**: This policy aligns with ISO 55001 standards to optimize asset management practices (Goncalves, T., 2024).

- **Key Sections to Include:**
    - **Intent and Scope**: Clearly define the objectives and coverage of the backup management policy.
    - **Principles and Responsibilities**: Outline principles for backup management and assign roles for implementation and oversight.
    - **Continual Improvement**: Commit to ongoing enhancement of backup management practices to meet evolving organizational needs (RedBeam, 2024).

Best Practices for Backup Management Compliance:

1. **Legal Compliance**: Ensure all backup practices adhere to legal and regulatory requirements, involving legal counsel in policy creation and reviews (Goncalves, T., 2024).
2. **Clear Communication**: Communicate backup policies clearly to all stakeholders to ensure understanding and compliance (RedBeam, 2024).
3. **Training and Awareness**: Conduct regular training sessions to educate employees on backup procedures and their importance in maintaining business continuity (Userflow, 2021).
4. **Regular Updates**: Periodically review and update backup policies to incorporate technological advancements and changes in organizational needs (Userflow, 2021).

Mapped Controls:

1. **Backup Definition and Scope:**
    - CSF Section and Sub-Category: ID.RA-1 Risk Assessment

- Related NIST 800-53v5 Controls: CP-2 Contingency Planning Policy and Procedures

2. **Benefits of Backup Management:**
    - CSF Section and Sub-Category: ID.RA-3 Continuous Monitoring
    - Related NIST 800-53v5 Controls: CP-9 Contingency Planning
3. **Policy Purpose and Importance:**
    - CSF Section and Sub-Category: PR.IP-12 Event-Driven Response
    - Related NIST 800-53v5 Controls: IR-4 Incident Handling
4. **Key Sections to Include:**

- **Intent and Scope:**
    - CSF Section and Sub-Category: PR.IP-1 Baseline Configuration
    - Related NIST 800-53v5 Controls: CM-2 Baseline Configuration
- **Principles and Responsibilities:**
    - CSF Section and Sub-Category: PR.AC-6 Security Training
    - Related NIST 800-53v5 Controls: AT-2 Security Awareness and Training
- **Continual Improvement:**
    - CSF Section and Sub-Category: PR.MA-3 Vulnerability Remediation
    - Related NIST 800-53v5 Controls: SI-2 Flaw Remediation

RACI Matrix:

Activity	**Responsible**	**Accountable**	**Consulted**	**Informed**
Define Backup Policy	IT Manager	CIO	Legal Counsel, Security Team	All Employees

Scope Identification	IT Manager	CIO	Department Heads	All Employees
Backup Schedule Implementation	Backup Administrator	IT Manager	Security Team	All Employees
Backup Testing	Backup Administrator	IT Manager	QA Team, Security Team	All Employees
Backup Storage Management	Backup Administrator	IT Manager	Security Team	All Employees
Policy Review and Updates	IT Manager	CIO	Legal Counsel, Security Team	All Employees
Training and Awareness	HR	IT Manager	Security Team	All Employees
Compliance Monitoring	Security Team	IT Manager	Legal Counsel, Internal Audit	All Employees
Incident Response for Backup Failures	IT Manager	CIO	Legal Counsel, Security Team	All Employees

Version Control:

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0		July 2024		Final Turn in and Approved Version
0.5	July 2024		700758100	No Changes needed

0.4	July 2024		700765919	No Changes needed
0.3	July 2024		700760007	Modified the Document
0.2	July 2024		Dr.M	APA isn't correct
0.1	July 2024		700760007	Initial Document creation

Logging Standard

Mohith Naga Adithya Vasamsetti

University of Central Missouri

700760007

Introduction:

Efficient logging is crucial for maintaining security, compliance, and operational efficiency in a company. This standard sets out rules and procedures for logging tasks in order to safeguard the integrity, availability, and confidentiality of log data.

Policy Elements:

Logging Definition and Scope:

- **Definition**: Logging involves the recording of events, transactions, and activities within information systems for monitoring and analysis purposes (Wickramage et al., 2019).
- **Scope:** This policy applies to all logging operations across the organization's systems, networks, and applications, including both on-premises and cloud environments.

How Logging Will Be Conducted:

- **Centralized Logging System**: Logs will all be gathered and saved in a single centralized logging system to simplify monitoring, analysis, and correlation.
- **Automated log Collection**: Automated log gathering will be conducted whenever feasible by utilizing tools and agents to gather log data from different origins.
- **Log Retention and Rotation**: Logs are required to be kept for at least one year to adhere to regulations and company policies. Log rotation is to be utilized for storage space management
- **Protection and Preservation of Log Integrity**: Logs will be safeguarded from unauthorized access and tampering by utilizing encryption and access controls.

- **Instantaneous Monitoring and Notifications**: Instant monitoring and notification systems will be implemented to promptly detect and address potential security incidents.

What Will Be Logged:

- **Access Logs**: It provides details on user interactions with systems, such as both successful and unsuccessful login attempts, length of sessions, and resources accessed.
- **System Logs:** Records of events created by the operating system, including system boot-up and shut-down, service errors, and modifications to system settings.
- **Application Logs**: They are events produced by applications such as user actions, e rror messages, and application initialization and termination.
- **Network Logs**: It contains details on network traffic, such as firewall logs, IDS/IPS logs, and VPN connections.
- **Security Logs**: Incidents involving security measures, like antivirus notifications, access modifications, and breaches of security regulations.

Benefits of Logging:

- **Security Monitoring**: Facilitates the detection and response to security incidents by providing detailed activity records (Torres et al., 2018).
- **Compliance and Audit**: Ensures adherence to regulatory requirements and supports audit activities through comprehensive log records (King, 2013).
- **Operational Insight**: Enhances the understanding of system behaviour and performance, aiding in troubleshooting and optimization (Wickramage et al., 2019).

Policy Purpose and Importance:

- **Objective**: To establish systematic guidelines for logging activities to ensure log data is available, accurate, and protected throughout its lifecycle.
- **Alignment:** This policy aligns with NIST SP 800-53 Rev. 5 controls and the NIST Cybersecurity Framework (CSF) to enhance security and compliance (NIST, 2020).

Key Sections to Include:

- **Intent and Scope**: Clearly define the objectives and coverage of the logging standard.
- **Principles and Responsibilities**: Outline principles for logging and assign roles for implementation and oversight.
- **Continual Improvement**: Commit to ongoing enhancement of logging practices to meet evolving organizational needs (Torres et al., 2018).

Mapped Controls:

1. Logging Definition and Scope:

- CSF Section and Sub-Category: DE.AE-1 Anomalies and Events
- Related NIST 800-53v5 Controls: AU-6 Audit Review, Analysis, and Reporting

2. Benefits of Logging:

- CSF Section and Sub-Category: PR.PT-1 Audit Logging
- Related NIST 800-53v5 Controls: AU-2 Event Logging

3. Policy Purpose and Importance:

- CSF Section and Sub-Category: PR.IP-12 Event-Driven Response

- Related NIST 800-53v5 Controls: IR-4 Incident Handling

4. Key Sections to Include:

- **Intent and Scope:**
  - CSF Section and Sub-Category: PR.IP-1 Baseline Configuration
  - Related NIST 800-53v5 Controls: CM-2 Baseline Configuration
- **Principles and Responsibilities:**
  - CSF Section and Sub-Category: PR.AC-6 Security Training
  - Related NIST 800-53v5 Controls: AT-2 Security Awareness and Training
- **Continual Improvement:**
  - CSF Section and Sub-Category: PR.MA-3 Vulnerability Remediation
  - Related NIST 800-53v5 Controls: SI-2 Flaw Remediation

Best Practices for Logging Compliance:

- **Legal Compliance**: Ensure all logging practices adhere to legal and regulatory requirements, involving legal counsel in policy creation and reviews (King, 2013).
- **Clear Communication**: Communicate logging policies clearly to all stakeholders to ensure understanding and compliance (Wickramage et al., 2019).
- **Training and Awareness**: Conduct regular training sessions to educate employees on logging procedures and their importance in maintaining security and compliance (Torres et al., 2018).
- **Regular Updates**: Periodically review and update logging policies to incorporate technological advancements and changes in organizational needs (Wickramage et al., 2019).

RACI Matrix:

Activity	Responsible	Accountable	Consulted	Informed
Define Logging Policy	IT Security Manager	CIO	Legal Counsel, Compliance Officer	All Employees
Identify Logging Scope	IT Security Manager	CIO	Department Heads, IT Team	All Employees
Implement Centralized Logging System	IT Team	IT Security Manager	Vendors, Security Team	All Employees
Manage Log Retention and Rotation	IT Team	IT Security Manager	Legal Counsel, Compliance Officer	All Employees
Ensure Log Integrity Protection	IT Security Manager	CIO	Security Team, IT Team	All Employees
Set Up Instant Monitoring and Notifications	IT Team	IT Security Manager	Security Team	All Employees
Policy Review and Updates	IT Security Manager	CIO	Legal Counsel, Compliance Officer	All Employees

Training and Awareness	HR	IT Security Manager	Security Team	All Employees

Version Control:

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0		July 2024		Final Turn in and Approved Version
0.5	July 2024		700758100	No Changes needed
0.4	July 2024		700765919	No Changes needed
0.3	July 2024		700760007	Modified the Document
0.2	July 2024		Dr.M	Don't bold citations
0.1	July 2024		700760007	Initial Document creation

Information Disposal Standard

Mohith Naga Adithya Vasamsetti

University of Central Missouri

700760007

Introduction:

Effective data disposal is crucial for upholding organizational security and adhering to regulatory mandates. This standard sets forth procedures and criteria for securely disposing of data and electronic media within the company.

Policy Elements:

Disposal Definition and Scope

- **Definition**: Disposal refers to the process of securely erasing or physically destroying electronic media to prevent unauthorized data recovery (Suthar et al., 2022).
- **Scope**: This policy applies to all electronic media, including hard disk drives (HDDs), solid-state drives (SSDs), and other storage devices, across the organization.

What Will Be Disposed

- **Data Types:** All sensitive, confidential, and personal data stored on electronic media.
- **Media Types**: HDDs, SSDs, tapes, CDs, DVDs, and other electronic storage devices.

How They Will Be Disposed

- **Data Destruction**: Implement guaranteed data destruction strategies, including overwriting, degaussing, and cryptographic erasure for HDDs and SSDs (Suthar et al., 2009).
- **Physical Destruction:** Employ shredding, crushing, or incineration to ensure that the media cannot be reused or reconstructed (Yan et al., 2013).

Disposal Standards

- **Compliance**: Adhere to the NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization, ensuring all disposal methods meet or exceed the recommended practices.

Audit Trail

- **Documentation:** Maintain detailed records of all disposal activities, including the type of media, method of destruction, date, and personnel involved.
- **Verification:** Conduct periodic audits to ensure compliance with the disposal standard and validate the effectiveness of data destruction methods.

Best Practices for Disposal Management Compliance:

1. **Legal Compliance**: Ensure all disposal practices adhere to legal and regulatory requirements, involving legal counsel in policy creation and reviews (Suthar et al., 2022).
2. **Clear Communication**: Communicate disposal policies clearly to all stakeholders to ensure understanding and compliance (Hughes et al., 2009).
3. **Training and Awareness**: Conduct regular training sessions to educate employees on disposal procedures and their importance in maintaining data security (Yan et al., 2013).
4. **Regular Updates**: Periodically review and update disposal policies to incorporate technological advancements and changes in organizational needs (Yan et al., 2013).

Mapped Controls:

1. Disposal Definition and Scope

- CSF Section and Sub-Category: ID.RA-1 Risk Assessment
- Related NIST 800-53v5 Controls: MP-6 Media Sanitization

2. What Will Be Disposed

- CSF Section and Sub-Category: PR.DS-3 Data-in-Transit Protection
- Related NIST 800-53v5 Controls: SC-28 Protection of Information at Rest

3. How They Will Be Disposed

- CSF Section and Sub-Category: PR. IP-6 Data Integrity
- Related NIST 800-53v5 Controls: MP-5 Media Transport

4. Disposal Standards

- CSF Section and Sub-Category: PR. IP-5 Data Destruction
- Related NIST 800-53v5 Controls: CP-9 Contingency Planning

5. Audit Trail

- CSF Section and Sub-Category: PR.PT-1 Audit Record Production
- Related NIST 800-53v5 Controls: AU-6 Audit Review, Analysis, and Reporting

RACI Matrix:

Task	Responsible	Accountable	Consulted	Informed
Disposal Definition and Scope	IT Security Team	Chief Information Officer (CIO)	Legal Team	All Employees

Identification of Data to be Disposed	IT Security Team	Data Protection Officer	Department Heads	All Employees
Selection of Disposal Method	IT Security Team	Chief Information Officer (CIO)	IT Vendor	All Employees
Data Destruction	IT Security Team	Chief Information Officer (CIO)	External Security Auditors	All Employees
Physical Destruction	IT Security Team	Chief Information Officer (CIO)	External Security Auditors	All Employees
Compliance with Disposal Standards	IT Security Team	Chief Information Officer (CIO)	Legal Team	All Employees
Maintaining Audit Trail	IT Security Team	Chief Information Officer (CIO)	Internal Audit Team	All Employees
Conducting Regular Audits	Internal Audit Team	Chief Information Officer (CIO)	External Auditors	IT Security Team
Training and Awareness	HR and IT Security Team	Chief Human Resources Officer	Training Consultants	All Employees
Policy Updates and Communication	IT Security Team	Chief Information Officer (CIO)	Legal Team, Department Heads	All Employees

Version Control:

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0		July 2024		Final Turn in and Approved Version
0.5	July 2024		700758100	No Changes needed
0.4	July 2024		700765919	No Changes needed
0.3	July 2024		700760007	Modified the Document
0.2	July 2024		Dr.M	Don't bold citations
0.1	July 2024		700760007	Initial Document creation

Procedure for Enabling and Forwarding Logging to

REDHAT-SIEM

Mohith Naga Adithya Vasamsetti

University of Central Missouri

700760007

Steps to configure logging:

The steps to configure logging on a Red Hat Enterprise Linux (RHEL) 8 server and forward these logs to REDHAT-SIEM, in accordance with our company's logging standard.

Server: Red Hat Enterprise Linux (RHEL) 8

Step 1: Install the Required Logging Tools

- First, make sure `rsyslog` is installed by using bash
    - sudo yum update -y
    - sudo yum install rsyslog -y

Step 2: Configure rsyslog for Remote Logging

- Edit the rsyslog configuration file to set up log forwarding to REDHAT-SIEM:
    - sudo nano /etc/rsyslog.conf
- Add the following line at the end of the file to define the remote server details:
    - *.* @@10.10.10.250:514
- This line tells rsyslog to forward all log messages to the SIEM at IP address 10.10.10.250 over TCP on port 514. The double at signs (@@) specify TCP, whereas a single at sign (@) would specify UDP.

Step 3: Enable and start rsyslog

- Ensure that rsyslog is enabled and running:
    - sudo systemctl enable rsyslog
    - sudo systemctl start rsyslog

Step 4: Verify rsyslog Configuration

- Check the rsyslog configuration for any errors:
    - sudo rsyslogd -N1
- This command tests the configuration file for syntax errors. If no errors are found, the output will indicate that the configuration is correct.

Step 5: Monitor Logs

- Verify that logs are being forwarded to the SIEM. Check the status of rsyslog:
    - sudo systemctl status rsyslog
- Additionally, confirm that logs are being received by REDHAT-SIEM.

Step 6: Set Up Log Rotation

- Ensure that log rotation is configured to manage log file sizes. Edit the logrotate configuration file:
    - sudo nano /etc/logrotate.conf
- Modify the configuration as needed to ensure logs are rotated and do not consume excessive disk space.

Step 7: Secure Logging Configuration

- Secure the rsyslog configuration file to prevent unauthorized changes:
    - sudo chown root:root /etc/rsyslog.conf
    - sudo chmod 600 /etc/rsyslog.conf

Step 8: Regular Review and Update

Regularly review and update the logging configuration to adapt to changes in organizational needs or compliance requirements, as specified in the "**Logging Standard Policy**."

By following these steps, you make sure that your server logs are sent correctly to REDHAT-SIEM, improving security monitoring and meeting the company's logging rules.

RACI Matrix:

Task	Responsible	Accountable	Consulted	Informed
Install Required Logging Tools	IT Administrator	IT Manager	System Security Team	CIO, Compliance Team
Configure rsyslog for Remote Logging	IT Administrator	IT Manager	System Security Team	CIO, Compliance Team
Enable and start rsyslog	IT Administrator	IT Manager	System Security Team	CIO, Compliance Team
Verify rsyslog Configuration	IT Administrator	IT Manager	System Security Team	CIO, Compliance Team
Monitor Logs	IT Administrator	IT Manager	System Security Team, SIEM Team	CIO, Compliance Team

Set Up Log Rotation	IT Administrator	IT Manager	System Security Team	CIO, Compliance Team
Secure Logging Configuration	IT Administrator	IT Manager	System Security Team	CIO, Compliance Team
Regular Review and Update	IT Administrator, IT Manager	IT Manager	Compliance Team	All Relevant Stakeholders

Version Control:

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0		July 2024		Final Turn in and Approved Version
0.5	July 2024		700758100	No Changes needed
0.4	July 2024		700765919	No Changes needed
0.3	July 2024		700760007	Modified the Document
0.2	July 2024		Dr.M	Don't bold citations
0.1	July 2024		700760007	Initial Document creation

Information Disposal Procedure

Mohith Naga Adithya Vasamsetti

University of Central Missouri

700760007

Introduction:

This process details the step-by-step method for securely disposing of electronic media following the **Information Disposal Standard**. The aim is to guarantee the permanent destruction of all sensitive, confidential, and personal data, while upholding organizational security and meeting regulatory obligations.

Procedure:

Disposal of Hard Disk Drives (HDDs)

1. Preparation

- Identify and label the HDDs designated for disposal.
- Connect the HDD to the sanitation machine.

2. Data Destruction

- Launch the sanitation program.
- Select the connected HDD from the list of available drives.
- Choose the appropriate wipe standard (e.g., 7-pass disk wipe) as per NIST SP 800-88 Rev. 1 guidelines (Regenscheid et al., 2015).
- Initiate the wipe process and monitor until completion (Yan et al.,2013).
- Verify that the sanitation program reports a successful wipe.

3. Physical Destruction

- Transfer the sanitized HDD to the physical destruction area.

- Employ shredding, crushing, or incineration methods (Kahn, 2018).
- Ensure the physical destruction process renders the HDD unrecoverable

4. Documentation

- Record the disposal activity, including:

  HDD serial number, Date of destruction, Method of destruction, Personnel involved

Mapped Controls:

1. Disposal Definition and Scope

- CSF Section and Sub-Category: ID.RA-1 Risk Assessment

2. What Will Be Disposed

- CSF Section and Sub-Category: PR.DS-3 Data-in-Transit Protection

3. How They Will Be Disposed

- CSF Section and Sub-Category: PR.IP-6 Data Integrity

4. Disposal Standards

- CSF Section and Sub-Category: PR.IP-5 Data Destruction

5. Audit Trail

- CSF Section and Sub-Category: PR.PT-1 Audit Record Production

RACI Matrix:

Task	Responsible	Accountable	Consulted	Informed
Preparation	IT Asset Management Team	IT Manager	Data Protection Officer	All Relevant Stakeholders
Data Destruction	IT Security Team	IT Manager	Data Protection Officer	Compliance Team
Physical Destruction	IT Security Team	IT Manager	Legal Team	All Relevant Stakeholders
Documentation	IT Asset Management Team	IT Manager	Compliance Team	All Relevant Stakeholders
Regular Review and Update	IT Security Team, Compliance Team	IT Manager	Legal Team	All Relevant Stakeholders

Version Control:

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0		July 2024		Final Turn in and Approved Version
0.5	July 2024		700758100	No Changes needed

0.4	July 2024		700765919	No Changes needed
0.3	July 2024		700760007	Modified the Document
0.2	July 2024		Dr.M	Don't bold citations
0.1	July 2024		700760007	Initial Document creation

Bring Your Own Device (BYOD) Guideline

Mohith Naga Adithya Vasamsetti

University of Central Missouri

700760007

Introduction:

Bring Your Own Device (BYOD) is becoming a more and more popular trend in today's digital world. Employees may use their personal devices, including laptops, tablets, and cell phones, for work as long as they follow this policy. BYOD poses serious security risks even if it can increase freedom and productivity. This policy describes if BYOD is acceptable in our company and offers suggestions based on best practices and recent research.

BYOD Policy Decision:

After thorough consideration, I believe that BYOD should be permitted in our organization, but with stringent security measures and policies in place. Allowing BYOD can improve employee satisfaction and productivity, reduce hardware costs, and support a flexible working environment. However, the potential risks necessitate a robust framework to safeguard our data and systems.

Key Considerations and Recommendations:

1. **Security Protocols**: Enforce rigorous security measures like encrypting data on personal devices, using robust passwords, and updating software regularly. These strategies safeguard sensitive data from unauthorized entry and cyber dangers (Yan et al., 2013).
2. **Access Control**: Restrict entry to sensitive data and systems according to the principle of granting minimum necessary access. Workers must only be given access to the information required for their specific job responsibilities. Adding multi-factor authentication (MFA) can provide an additional level of security (Herrera et al., 2017).

3. **Monitoring and Management**: Use mobile device management (MDM) solutions to monitor and manage all personal devices accessing the corporate network. MDM can enforce security policies, remotely wipe data from lost or stolen devices, and ensure compliance with organizational standards (Dillon, 2013).
4. **Training and Awareness**: Conduct regular training sessions to educate employees about the risks associated with BYOD and the importance of following security protocols. Awareness programs can significantly reduce the likelihood of security breaches due to human error (Yan et al., 2013).
5. **Legal and Compliance Issues**: Ensure that the BYOD policy complies with all relevant legal and regulatory requirements. This includes data protection laws, industry standards, and corporate governance policies (Dillon, 2013).

Mapped Controls:

1. **Security Protocols:**
    - CSF Section and Sub-Category: PR.DS-1 (Data-at-Rest Protection)
    - Related NIST 800-53v5 Controls: SC-12 (Cryptographic Key Establishment and Management), SC-13 (Cryptographic Protection)
2. **Access Control:**
    - CSF Section and Sub-Category: PR.AC-1 (Identity Management, Authentication and Access Control)
    - Related NIST 800-53v5 Controls: AC-2 (Account Management), AC-3 (Access Enforcement)

3. **Monitoring and Management:**
    - CSF Section and Sub-Category: DE.CM-1 (Security Continuous Monitoring)
    - Related NIST 800-53v5 Controls: CA-7 (Continuous Monitoring), SI-4 (System Monitoring)
4. **Training and Awareness:**
    - CSF Section and Sub-Category: PR.AT-1 (Awareness and Training)
    - Related NIST 800-53v5 Controls: AT-2 (Awareness Training), AT-3 (Role-Based Training)
5. **Legal and Compliance Issues:**
    - CSF Section and Sub-Category: ID.GV-3 (Governance and Privacy)
    - Related NIST 800-53v5 Controls: PM-8 (Critical Infrastructure Plan), PL-1 (Security Planning Policy and Procedures)

RACI Matrix:

Task	**Responsible**	**Accountable**	**Consulted**	**Informed**
Develop BYOD Policy	IT Security Team	CIO	Legal Department	All Employees
Implement Security Protocols	IT Security Team	CIO	IT Department	All Employees
Monitor and Manage Devices	IT Security Team	CIO	IT Department	All Employees

Task	Responsible	Accountable	Consulted	Informed
Conduct Training Sessions	HR Department	HR Director	IT Security Team	All Employees
Ensure Legal Compliance	Legal Department	Legal Counsel	IT Security Team, HR Dept	All Employees

Version Control:

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0		July 2024		Final Turn in and Approved Version
0.3	July 2024		700758100	No Changes needed
0.2	July 2024		700765919	No Changes needed
0.1	July 2024		700760007	Initial Document creation

Company Use of ChatGPT: Guideline

Mohith Naga Adithya Vasamsetti

University of Central Missouri

700760007

Introduction:

ChatGPT, an advanced language model developed by OpenAI, has revolutionized various sectors by enhancing productivity and providing automated support. As a subject matter expert, this guideline aims to provide explicit recommendations on whether the company should integrate ChatGPT into its operations.

Guideline on ChatGPT Usage:

1. Permitted Use Cases:

ChatGPT should be used in scenarios where it can significantly enhance efficiency and productivity without compromising data security or confidentiality. These use cases include:

- **Customer Support**: Automating responses to common queries can reduce the workload on customer support teams and ensure quick resolution times (Thompson & Lee, 2023).
- **Content Generation**: Assisting in drafting documents, generating reports, and creating content for marketing purposes can save valuable time (Thompson & Lee, 2023).
- **Internal Communication**: Streamlining internal communication through automated message drafting and summarization can improve clarity and reduce time spent on routine tasks (Thompson & Lee, 2023).

2. Restricted Use Cases:

While ChatGPT offers numerous benefits, its use must be restricted in certain scenarios to safeguard sensitive information and ensure compliance with regulatory standards. These restrictions include:

- **Confidential Information**: ChatGPT should not be used to process or handle any confidential or sensitive company data. This includes customer data, financial information, and proprietary business strategies (Cheng, 2023).
- **Decision-Making**: Automated systems should not make critical business decisions without human oversight. ChatGPT can provide insights and suggestions, but final decisions should rest with human experts (Cheng, 2023).
- **Regulatory Compliance**: Any use of ChatGPT must comply with industry regulations and standards to avoid legal repercussions (Cheng, 2023).

3. Training and Monitoring:

To ensure the effective and ethical use of ChatGPT, the company should implement the following measures:

- **Employee Training**: Staff should be trained on the appropriate use of ChatGPT, focusing on maximizing its benefits while adhering to company policies and ethical standards (Smith & Zhao, 2023).
- **Regular Monitoring**: Continuous monitoring of ChatGPT's outputs is essential to ensure accuracy, relevance, and adherence to company guidelines. Regular audits should be conducted to identify and rectify any misuse or errors (Smith & Zhao, 2023).

Mapped Controls:

1. **Permitted Use Cases**
    - CSF Section and Sub-Category: ID.AM-1: Asset Management
2. **Restricted Use Cases**
    - CSF Section and Sub-Category: PR.AC-5: Access Control

3. **Training and Monitoring**
    - CSF Section and Sub-Category: PR.AT-1: Awareness and Training

RACI Matrix:

Task	Responsible	Accountable	Consulted	Informed
Develop ChatGPT Usage Policy	IT Security Team	CIO	Legal, Compliance	All Employees
Implement ChatGPT in Customer Support	Customer Support Team	Head of Customer Support	IT Security Team	All Employees
Monitor ChatGPT Outputs	IT Security Team	CIO	Legal, Compliance	All Employees
Conduct Employee Training	HR Team	Head of HR	IT Security Team	All Employees
Regular Audits and Reviews	Internal Audit Team	CFO	IT Security Team	Board of Directors

Version Control:

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0		July 2024		Final Turn in and Approved Version
0.3	July 2024		700758100	No Changes needed

0.2	July 2024		700765919	No Changes needed
0.1	July 2024		700760007	Initial Document creation

Incident Response Plan for Lost/Stolen Laptop Containing ePHI

Mohith Naga Adithya Vasamsetti

University of Central Missouri

700760007

Introduction:

This plan details the steps to take if a laptop with ePHI is lost or stolen. The plan aims to adhere to HIPAA and other regulations, while reducing the incident's possible consequences.

Incident Identification and Initial Response:

- **Incident Reporting:**
    - Immediately report the loss or theft of the laptop to the organization's IT security team and management (Miller, 2016).
    - Provide details such as the date, time, and location of the incident, along with any other relevant information (Jerbic et al., 2007).
- **Information Gathering:**
    - Determine whether the laptop contained ePHI and if so, assess the extent of the data involved (Scarfone et al., 2007).
    - Confirm whether the laptop was encrypted and if additional security measures (e.g., remote wipe capability) were in place (Miller, 2016).

Initial Containment:

- If the laptop is confirmed to contain ePHI, initiate measures to prevent unauthorized access to the data. This may include disabling remote access and triggering a remote wipe if possible (Jerbic et al., 2007).

Investigation and Assessment:

- **Investigation:**
    - Conduct a thorough investigation to gather all necessary details about the incident. This includes identifying who had access to the laptop, the security controls in place, and any potential witnesses (Miller, 2016).
    - Obtain a police report if the laptop was stolen, documenting the incident for legal and compliance purposes (Scarfone et al., 2007).
- **Risk Assessment:**
    - Evaluate the potential risks associated with the loss or theft, including the likelihood of unauthorized access to ePHI and the possible impact on patients and the organization (Miller, 2016).
    - Determine if the incident triggers breach notification requirements under HIPAA or other regulations (Jerbic et al., 2007).

Notification and Communication:

- **Internal Communication:**
    - Inform all relevant internal stakeholders, including senior management, legal, and compliance teams, about the incident and the steps being taken in response (Scarfone et al., 2007).
- **Notification:**
    - Notify affected individuals if there is a significant risk that their ePHI has been compromised. Include details about the incident, the information involved, and steps they can take to protect themselves (Miller, 2016).

- Notify relevant regulatory bodies as required by law (Jerbic et al., 2007).

Remediation and Recovery:

- **Remediation:**
  - Implement corrective actions to address any identified vulnerabilities that contributed to the incident. This may include enhancing security protocols, updating policies, and providing additional training to staff. (Miller, 2016).
- **Recovery:**
  - Restore affected systems and processes to normal operations, ensuring that any compromised data is secured and that similar incidents are prevented in the future (Jerbic et al., 2007).

Post-Incident Review:

- Conduct a post-incident review to evaluate the effectiveness of the response and identify areas for improvement. Update the incident response plan as necessary (Scarfone et al., 2007).

RACI Matrix:

Activity	Responsible	Accountable	Consulted	Informed
Incident Reporting	Employee	IT Security Manager	IT Security Team	Senior Management

Information Gathering	IT Security Team	IT Security Manager	Compliance Team	Legal Team
Investigation	IT Security Team	Incident Response Coordinator	Legal Team, Compliance Team	Senior Management
Risk Assessment	Compliance Team	Chief Information Security Officer (CISO)	IT Security Team	Senior Management
Notification (Internal/External)	IT Security Manager	CISO	Legal Team, Compliance Team	Affected Individuals, Regulatory Bodies
Remediation	IT Security Team	CISO	IT Department, Compliance Team	Senior Management
Recovery	IT Department	IT Security Manager	Compliance Team	All Employees
Post-Incident Review	IT Security Team	Incident Response Coordinator	Legal Team, Compliance Team	Senior Management

Mapped CSF Controls:

1. Incident Reporting

- CSF Section and Sub-Category: ID.AM-5: Asset Management

2. Information Gathering and Investigation

- CSF Section and Sub-Category: PR.DS-1: Data Security

3. Risk Assessment

- CSF Section and Sub-Category: ID.RA-1: Risk Assessment

4. Notification and Communication

- CSF Section and Sub-Category: RS.CO-1: Communications

5. Remediation and Recovery

- CSF Section and Sub-Category: RC.RP-1: Recovery Planning

6. Post-Incident Review

- CSF Section and Sub-Category: RC.IM-1: Improvements

Version Control:

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0		July 2024		Final Turn in and Approved Version
0.3	July 2024		700758100	No Changes needed

0.2	July 2024		700765919	No Changes needed
0.1	July 2024		700760007	Initial Document creation

References:

1. Asset Management Policy. (2021). Userflow https://userflow.com/policies/security/asset-management
2. Cheng, X. (2023). Ethical implications of AI in corporate environments. Journal of Applied Science and Computation, 12(3), 456-470. https://doi.org/10.1016/j.jasc.2023.07.001
3. Dillon, T. (2013). Protecting BYOD environments. Procedia Technology, 9, 234-238. https://doi.org/10.1016/j.protcy.2013.12.005
4. Frsecure. (n.d.). Acceptable use policy. https://frsecure.com/acceptable-use-policy-template/
5. Goncalves, T. (2024). A complete guide to building an asset management policy. Goncalves, T. https://fiixsoftware.com/blog/asset-management-policy-complete-guide/
6. Herrera, A. V., Ron, M., & Rabadão, C. (2017). National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In 2017 12th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-4). IEEE. https://doi.org/10.23919/CISTI.2017.7975953
7. How to Build an Asset Management Policy (2024). Redbeam https://redbeam.com/blog/build-an-asset-management-policy#:~:text=An%20asset%20management%20policy%20can,purchase%20to%20maintenance%20to%20disposal.
8. Hughes, G. F., Coughlin, T., & Commins, D. M. (2009). Disposal of Disk and Tape Data by Secure Sanitization. IEEE Security & Privacy, 7(4), 29-34. https://doi.org/10.1109/MSP.2009.89

9. Jerbic, S. M., & Wu, S. S. (2007). The Security Rule. In A guide to HIPAA security and the law (pp. 25-92). https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1046&context=econ_pub
10. Kahn, R. A. (2018). Why destruction of information is so difficult and so essential: The case for defensible disposal. IQ: The RIM Quarterly, 34(4), 24–27 https://search.informit.org/doi/10.3316/ielapa.965963253537406
11. King, J. (2013). Logging in healthcare: Building a better audit trail. In Proceedings of the USENIX Healthtech Conference. https://www.usenix.org/system/files/conference/healthtech13/healthtech13-king.pdf
12. Kirvan, P. (n.d.). Acceptable use policy (AUP). TechTarget. https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP
13. Miller, J. (2016). EPHI leak risks and legal concerns for BYOD in a healthcare environment (Order No. 10109628). ProQuest One Academic. (1796238133) https://login.cyrano.ucmo.edu/login?url=https://www.proquest.com/dissertations-theses/ephi-leak-risks-legal-concerns-byod-healthcare/docview/1796238133/se-2
14. National Institute of Standards and Technology (NIST). (2020). NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5
15. Regenscheid, A., Feldman, L., & Witte, G. (2015). NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD. [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=917935

16. Scarfone, K. A., Souppaya, M. P., & Sexton, M. (2007). Guide to storage encryption technologies for end user devices (NIST Special Publication 800-111). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-111
17. Scheldt, A. (2024). Security awareness training: Why you need a corporate acceptable use policy. CompTIA. https://www.comptia.org/blog/security-awareness-training-corporate-acceptable-use-policy
18. Smith, J., & Zhao, L. (2023). Legal considerations for AI deployment in the workplace. Open Human Nature Journal, 15(2), 320-335. https://doi.org/10.1002/ohn.720
19. Suthar, H., & Sharma, P. (2022). Guaranteed Data Destruction Strategies and Drive Sanitization: SSD, 01 August 2022, PREPRINT (Version 1) available at Research Square. https://doi.org/10.21203/rs.3.rs-1896935/v1
20. Thompson, R., & Lee, H. (2023). Risk management strategies for AI technologies in business. SSRN Electronic Journal. https://dx.doi.org/10.2139/ssrn.4514238
21. Torres, C., Fried, J. C., & Manjunath, B. S. (2018). Healthcare event and activity logging. IEEE Journal of Translational Engineering in Health and Medicine, 6, 1-12. https://doi.org/10.1109/JTEHM.2018.2863386
22. Wickramage, C., Fidge, C., Ouyang, C., & Sahama, T. (2019). Generating log requirements for checking conformance against healthcare standards using workflow modelling. In Proceedings of the Australasian Computer Science Week Multiconference (Article 35, 1–10). Association for Computing Machinery. https://doi.org/10.1145/3290688.3290739
23. Yan, G., Xue, M., & Xu, Z. (2013). Disposal of waste computer hard disk drive: data destruction and resources recycling. Waste Management & Research, 31(6), 559–567. https://doi.org/10.1177/0734242X13481085

24. Yan, G., Xue, M., & Xu, Z. (2013). Ensuring data security in BYOD environments. International Journal of Medical Informatics, 117, 99-108. https://doi.org/10.1016/j.ijmedinf.2018.09.013

25. Yan, G., Xue, M., & Xu, Z. (2013). Techniques and Challenges in Secure Data Destruction. Journal of Computer Security, 21(1), 34-50. http://dx.doi.org/10.24423/cames.2024.492