Standard Operating Procedures

Night Owl Network

Table Of Contents

Employee Onboarding SOP

Author: Geneva Knott

Purpose:

The Purpose of this procedure is to develop a plan for providing technology resources to new employees, including hardware, software and system access

Scope:

Inform all relevant stakeholders, Including IT personnel and HR, about the plan and any requirements for handling technology assets.

Responsibilities:

The IT department is responsible for implementing, following, reviewing, maintaining, and updating this policy in conjunction with company specifications.

Prerequisites:

Identify all technology assets that will be assigned to the new employee including laptops, mobile devices, and other company owned equipment. Identify all software and systems to which the new employee will need access, including email accounts, cloud storage and other online tools.

Procedure:

Asset Allocation: Allocate the necessary technology assets to the new employee as identified in prerequisites.

Software and Access Provisioning: Provision access to all software and systems to which the new employee will need access, including email accounts, cloud storage, and other online tools.

Data Migration: Ensure all necessary data is migrated from the previous employees technology assets, including email, files and other relevant data.

Data Transfer: Transfer any relevant data or files from the new employees personal technology assets to their company-owned assets.

Training: Provide training to new employees on how to use technology assets and software to perform their job function.

Support: Provide ongoing support to the new employee for any technology related issues or questions.

Documentation: Document all technology assets assigned to new employees, date of allocation, and any relevant training or support provided.

Compliance: Ensure that all documentation and procedures are compliant with relevant regulations and company policies.

References:

- https://blog.netwrix.com/2018/06/07/how-to-create-new-active-directory-users-with-powershell/
- https://adamtheautomator.com/powershell-onboarding-script/

Revision History:

04/03/2023 -- "Handling Technology for Onboard” created by Geneva Knott

Employee Off-Boarding SOP:

Author: Geneva Knott

Purpose:

The purpose of this procedure is to establish a trusted procedure to identify all technology assets assigned to the employee, including laptops, mobile devices, and other company-owned equipment. Identify all software and systems to which the employee has access. Including email accounts, cloud storage, and other online tools. Once identified establishing the appropriate termination of all access and collection of the property.

Scope:

These procedures apply to all relevant stakeholders, including IT personnel and HR, about the plan and any requirements for handling technology assets.

Responsibilities:

The IT department is responsible for implementing, following, reviewing, maintaining, and updating this policy in conjunction with company specifications.

Prerequisites:

Identify all technology assets that will be assigned to the new employee including laptops, mobile devices, and other company owned equipment. Identify all software and systems to which the new employee will need access, including email accounts, cloud storage and other online tools

Procedure:

Collection of Assets: On the day of the termination, collect all technology assets assigned to the employee, including laptops, mobile devices, and other company owned equipment.

Disabling Access: Disable access to all software and systems to which the employee has access, including email accounts, cloud storage, and other online tools

Data Backup:Ensure all important data on the employees technology assets is backed up before the assets are wiped and repurposed.

Archiving: Archive any relevant data or files for future reference or compliance requirements.

Wiping and Disposal: Wipe all company data from the employees technology assets and dispose of the assets in accordance with company policies and regulations.

Record Keeping: Document all technology assets assigned to the employee, date of collection, and the disposition of the assets.

Compliance: Ensure that all documentation and procedures are compliant with relevant regulations and company policies.

References:

- https://asana.com/resources/employee-offboarding
- https://blog.netwrix.com/2018/06/07/how-to-create-new-active-directory-users-with-powershell/

Revision History:

04/03/2023 -- "Onboarding" created by Geneva Knott

OS Version Control SOP:

Author: Nick Alderete

Purpose:

This Standard Operating Procedure (SOP) is designed to provide guidelines for the version control and updating of operating systems (OS) on all devices connected to the network. The purpose of this SOP is to ensure that all devices on the network have the latest OS version and security updates, and that the process is managed in a controlled and consistent manner, with clear roles and responsibilities defined for all involved parties.

Scope:

This SOP applies to all devices connected to the network, including but not limited to servers, workstations, laptops, and mobile devices. This SOP covers all operating systems, including Windows, macOS, Linux, and mobile OSes.

Responsibilities:

The following roles and responsibilities are defined for the version control and updating of operating systems:

- IT Manager: responsible for reviewing and approving OS updates, coordinating update implementation, and ensuring updates are completed as per the defined procedures.
- System Administrator: responsible for scheduling and implementing OS updates, testing updates, and verifying that the updates have been successfully completed.
- End User: responsible for ensuring that their device is connected to the network during the scheduled update window, and for reporting any issues to the System Administrator

Prerequisites:

Before updating any operating system, the following prerequisites must be met:

- OS update: A formal OS update request must be submitted and approved by the IT Manager.
- Testing: Testing must be conducted in a testing environment before implementing updates in the production environment.
- Backups: All affected devices must be backed up before the OS update implementation.
- Communication plan: A communication plan must be established, including notifying all stakeholders of the update and scheduling a maintenance window.

Procedure:

The following procedures must be followed when version controlling and updating operating systems:

- OS update request: The System Administrator submits a formal OS update request to the IT Manager, including all relevant details such as the reason for the update, the expected impact, and the proposed implementation plan.
- OS update review: The IT Manager reviews the OS update request and approves it based on the defined criteria, such as the impact on the network, the availability of resources, and the potential risks.
- Testing: The System Administrator conducts testing in a testing environment to ensure that the OS update works as expected and does not negatively impact the device or the network.
- OS update implementation: The System Administrator implements the OS update during the scheduled maintenance window, following the implementation plan and verifying that the update has been successfully completed.
- Documentation: The IT Manager documents all OS updates, including the reason for the update, the implementation plan, testing results, and post-update review results.

References:

- https://www.atlassian.com/git/tutorials/what-is-version-control#:~:text=Version%20control%2C%20also%20known%20as,to%20source%20code%20over%20time.

Revision History:

4/5/2023 - “OS Control” - Nick A

File Sharing SOP:

Author: Connie Uribe Chavez

Purpose:

The purpose of this s Standard Operating Procedure (SOP) is to define Active Directory file permissions management. To provide step-by-step instructions to IT Administrators on how to maintain the file sharing and to ensure the security, integrity, and confidentiality of the data.

Scope:

CleanPower team of engineers and energy experts will be granted persmission after they read and sign the File Sharing User Acceptance Agreement. The Night Owl Network IT Administrator will be granting permissions.

Responsibilities:

Night Owls Network Administrators will be in charge of granting access, modifying permissions, and revoking access to the file share.

- Data owners are responsible for identifying the sensitivity and classification level of the data and granting access accordingly.
- Data custodians are responsible for maintaining the integrity and confidentiality of the data and ensuring that access is granted only to authorized personnel.
- System administrators are responsible for implementing and maintaining the access control mechanisms.

Prerequisites:

- Data owners must classify the data based on sensitivity and confidentiality level.
- Personnel involved in file access must be trained on the use of the access control mechanisms.
- Cyber security training for employees wanting access. This training should be provided by the Night Owl Network team.
- Read and sign the File Sharing User Acceptance Agreement provided by Night Owl Network.

Procedure:

Night Owl Network is responsible for the overall management and development the directory and subdirectory structure on the shared drives.

1. The IT administrators will setup the shared drive.

2. Employees on the roster should be added to the shared drive. Identify the data owner: Before requesting access to a file, identify the data owner and verify that you are authorized to access the data.
3. The IT administrators will ensure all functionalities are funtioning.
4. The IT administrators must backup the Shared Drive daily.
5. To ensure security, HR must email the names of new employees that will be granted permission to the shared drive to the IT department
6. New employees must complete all the prerequesites before they are given any access to the shared drive.
7. Information stored on the shared drive must follow CleanPower company guidelines.

The following procedures must be followed to access files on the Night Owl Network: a. Identify the data owner: Before requesting access to a file, identify the data owner and verify that you are authorized to access the data. b. Request access: Submit a request for access to the data owner or the designated custodian. The request should include the reason for access, the duration of access, and the classification level of the data. c. Verify access: The data owner or designated custodian will verify your request and grant access based on the sensitivity and classification level of the data. d. Access the file: Once access is granted, access the file using the designated access control mechanisms. e. Monitor access: The system administrator will monitor access to the file to ensure that it is accessed only by authorized personnel and to detect any potential security breaches. f. Terminate access: When access is no longer required, terminate access using the designated access control mechanisms.

Definitions:

Shared drive(s) - file being shared between employees on the approved roster.

Policy

SOP -- This policy will take into effect once the Active Directory for CleanPower takes place and it will stay in effect until further revisions. Work Instructions -- Night Owl Network will have their own guidelines on how to setup the shared drive to ensure full security.

References:

https://support.microsoft.com/en-us/windows/-windows-file-system-access-and-privacy-a7d90b20-b252-0e7b-6a29-a3a688e5c7be#:~:text=How%20the%20file%20system%20access,file%20system%20is%20turned%20On.

Revision History:

04/03/2023 -- "SOP Google Doc" created by Connie Uribe Chavez
04/05/2023 -- "File Access.md" created by Connie Uribe Chavez

Monitoring Network Traffic SOP:

Author: Connie Uribe Chavez

Purpose:

The purpose of this SOP is to establish guidelines for monitoring network traffic on the cleanpower to ensure the security and reliability of the network.

This document will answer the question "How will you write and organize your SOPs?" while also serving as an example of the format.

Scope:

This SOP applies to all personnel who have access to the CleanPower network and are responsible for monitoring network traffic.

Responsibilities:

The following are the responsibilities of the personnel involved in monitoring network traffic:

Network administrators are responsible for configuring the network monitoring tools and ensuring that they are functioning properly.
Security analysts are responsible for analyzing network traffic to detect any potential security threats or breaches.
IT support staff are responsible for responding to any network issues reported by the network monitoring tools.

Prerequisites:

The following prerequisites must be met before implementing this SOP:

- Network monitoring tools must be installed and configured on the Night Owl Network.
- Personnel involved in monitoring network traffic must be trained on the use of the network monitoring tools.

Procedure:

The following procedures must be followed to monitor network traffic on the CleanPower Network:

1. Configure network monitoring tools: Network administrators must configure the network monitoring tools to capture all network traffic and store it in a centralized location for analysis.

2. Monitor network traffic: Security analysts must regularly review the network traffic logs to identify any potential security threats or breaches. They should also review logs in response to any suspicious activity reported by the monitoring tools.
3. Analyze network traffic: Security analysts must analyze the network traffic logs to determine the nature and severity of any security threats or breaches. They should also document their findings and notify the appropriate personnel of any significant incidents.
4. Respond to network issues: IT support staff must respond to any network issues reported by the monitoring tools in a timely manner. They should also document their actions and communicate with network administrators and security analysts as needed.

Policy

SOP -- Traffic monitoring should be done on a daily basis or more oftern if needed. Work Instructions
Configuring Network Monitoring Tools

- Launch the network monitoring tool and log in using your credentials.
- Select the appropriate network interface(s) to capture traffic.
- Set filters to capture only the traffic of interest.
- Configure the storage location and retention policy for captured traffic.
- Set up alerts to notify security analysts of suspicious activity.

Monitoring Network Traffic

- Log in to the network monitoring tool and select the appropriate interface(s) to monitor.
- Review the real-time traffic dashboard to identify any anomalies or suspicious activity.
- Review the network traffic logs on a regular basis to identify any patterns or trends.
- Investigate any suspicious activity and escalate as necessary.

Analyzing Network Traffic

- Open the network traffic logs in the network monitoring tool.
- Filter the logs to display only the relevant traffic.
- Analyze the traffic to identify any security threats or breaches.
- Document your findings and notify the appropriate personnel.

Responding to Network Issues

- Log in to the network monitoring tool and review any alerts or notifications.
- Investigate any reported issues and attempt to resolve them.
- Escalate any unresolved issues to the appropriate personnel.
- Document your actions and communicate with network administrators and security analysts as needed.

References:

NIST Guidelines on Firewalls and Firewall Policy
Cloud Security Attacker Techniques, Monitoring, and Threat Detection
CIS Critical Security Control

Revision History:
04/05/2023 -- "Monitoring Network Traffic.md" created by Connie Uribe Chavez 04/06/2023 -- "Monitoring Network Traffic.md" edited by Connie Uribe Chavez

Networking Changes SOP:

Author: Nick Alderete

Purpose:

This Standard Operating Procedure (SOP) is designed to provide guidelines for managing changes to the network, including hardware, software, or configuration changes, with the primary goal of minimizing disruptions and downtime. The purpose of this SOP is to ensure that changes are implemented in a controlled and consistent manner, with clear roles and responsibilities defined for all involved parties.

Scope:

This SOP applies to all network changes, including but not limited to changes to network hardware, software, configuration, and security measures. This SOP covers all network changes made to production, development, and testing environments.

Responsibilities:

The following roles and responsibilities are defined for managing network changes:

- Network Administrator: responsible for reviewing and approving network change requests, coordinating change implementation, and ensuring changes are completed as per the defined procedures.
- Change Requestor: responsible for submitting network change requests, providing all relevant details, and reviewing the implementation plan.
- Change Reviewer: responsible for reviewing the implementation plan and verifying that the change has been successfully completed.

Prerequisites:

Before implementing any network changes, the following prerequisites must be met:

- Change request: A formal change request must be submitted and approved by the Network Administrator.
- Implementation plan: A detailed implementation plan must be created, including a rollback plan in case of issues.
- Backups: All affected network devices must be backed up before the change implementation.
- Testing: Testing must be conducted in a development or testing environment before implementing changes in the production environment.

Procedure:

The following procedures must be followed when managing network changes:

- Change request submission: The Change Requestor submits a formal change request to the Network Administrator, including all relevant details such as the reason for the change, the expected impact, and the proposed implementation plan.
- Implementation plan creation: The Change Implementer creates a detailed implementation plan, including the steps required to implement the change, the resources required, and a rollback plan in case of issues.
- Testing: The Change Implementer conducts testing in a development or testing environment to ensure that the change works as expected and does not negatively impact the network.
- Communication plan: The Network Administrator establishes a communication plan to notify all stakeholders of the change, including the scheduled maintenance window, and any potential impact or downtime.
- Change implementation: The Change Implementer implements the change during the scheduled maintenance window, following the implementation plan and verifying that the change has been successfully completed.
- Documentation: The Network Administrator documents all network changes, including the reason for the change, the implementation plan, testing results, and post-implementation review results

References:

- https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-role-of-networks-in-organizational-change

Revision History:

4/5/2023 - “Networking Changes” -Nick A

Management and maintaining the Network SOP:

Author: Sierra Maldonado

Purpose:

The purpose of this SOP is to establish a set of guidelines for managing and maintaining the network.

Scope:

This SOP applies to all members of the IT department responsible for network management and maintenance.

Responsibilities:

a. IT Manager: The IT manager is responsible for overseeing the network management and maintenance procedures, ensuring that the SOP is up-to-date, and providing support to the IT team as needed.

b. Network Administrator: The network administrator is responsible for implementing and maintaining the network infrastructure, including switches, routers, firewalls, and other network devices. The administrator will also manage user accounts and permissions, monitor network traffic, and troubleshoot issues as they arise.

c. Help Desk Technician: The help desk technician is responsible for assisting end-users with network-related issues. They will document reported issues, escalate complex issues to the network administrator, and follow up with end-users to ensure that issues are resolved.

Prerequisites:

Training and Awareness:
Training: All members of the IT department responsible for network management and maintenance must receive regular training to stay up-to-date with industry best practices and new technologies.
Awareness: End-users must be made aware of network policies, security measures, and best practices to ensure that they are using the network in a safe and secure manner.

Procedure:

- Maintenance
- Verify the performance of the network and all internetwork devices in the network
- Baseline the performance of the network itself
- Understand the amount of direction and traffic flows in the network
- Identify and troubleshoot potential network issues

1) Approval: All changes to the network, including device configurations, software updates, and security policy changes, must be approved by the IT manager before implementation.
2) Documentation: All changes must be documented in the centralized documentation system, including the reason for the change, the proposed solution, and any potential impacts on the network.
3) Testing: Changes must be tested in a non-production environment before implementation to ensure that they do not cause any adverse effects on the network or end-users.
4) Implementation: Changes will be implemented during a predetermined maintenance window to minimize disruption to end-users.

References:

- https://www.techtarget.com/searchnetworking/tip/Key-tasks-in-a-network-maintenance-checklist
- https://www.howtonetwork.org/tshoot/module-1/network-maintenance-tasks/

Revision History:

04/05/2023 - “Management and Maintenance” - Sierra