Standard Operating Procedures

Night Owl Network

Table Of Contents

Handling Technology for Onboard

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 Access SOP:

Author: Connie Uribe Chavez

Purpose:

The purpose of this SOP is to define Active Directory file permissions management.

Scope:

[What areas of the organization will be affected.]

Responsibilities:

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

Prerequisites:

[The information, resources, permissions, etc. required to execute this procedure.]

Procedure:

[The outline of the activities or sequence of steps for performing the procedure. This should not be overly detailed -- let it capture the shape of the activity to be performed, regardless of how the details of its implementation might change.]

- Begin with a flow chart map of the parts of the procedure being defined. This will become your outline
- Bundle closely related tasks together for concision, especially if they always occur together/in sequence without much deviation
- Work to have 5-7 tasks -- too few and it's not worth reading; too many and it's too hard to read. This is about parsing.
- Now revise the flowchart to match the way you have bundled steps and number each steps
- Write a concise, focused description for each step
- Add a brief opening overview paragraph to describe the topic , inputs, outputs, expected results, and involved roles

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

Monitoring Network Traffic SOP:

Author: Connie Uribe Chavez

Purpose:

[The purpose or rationale for the procedure. If there are policies or standards which this procedure exists to meet, reference them here.]

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

Scope:

[What areas of the organization will be affected.]

Responsibilities:

[Who is responsible for implementing, following, reviewing, maintaining, and updating this policy.]

Prerequisites:

[The information, resources, permissions, etc. required to execute this procedure.]

Procedure:

[The outline of the activities or sequence of steps for performing the procedure. This should not be overly detailed -- let it capture the shape of the activity to be performed, regardless of how the details of its implementation might change.]

- Begin with a flow chart map of the parts of the procedure being defined. This will become your outline
- Bundle closely related tasks together for concision, especially if they always occur together/in sequence without much deviation
- Work to have 5-7 tasks -- too few and it's not worth reading; too many and it's too hard to read. This is about parsing.
- Now revise the flowchart to match the way you have bundled steps and number each steps
- Write a concise, focused description for each step
- Add a brief opening overview paragraph to describe the topic , inputs, outputs, expected results, and involved roles

References:

- https://www.teramind.co/blog/ways-to-monitor-network-traffic/#:~:text=What%20Is%20Network%20Traffic%20Monitoring,understanding%20of%20overall%20network%20activity.

Revision History:

2/12/2021 -- "SOP_Template.md" created by Ethan Denny

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