SOP:Handling Network Accounts for Onboarding Employees

Purpose:

The purpose of this Standard Operating Procedure (SOP) is to outline the process for handling network accounts for onboarding new employees in our organization.

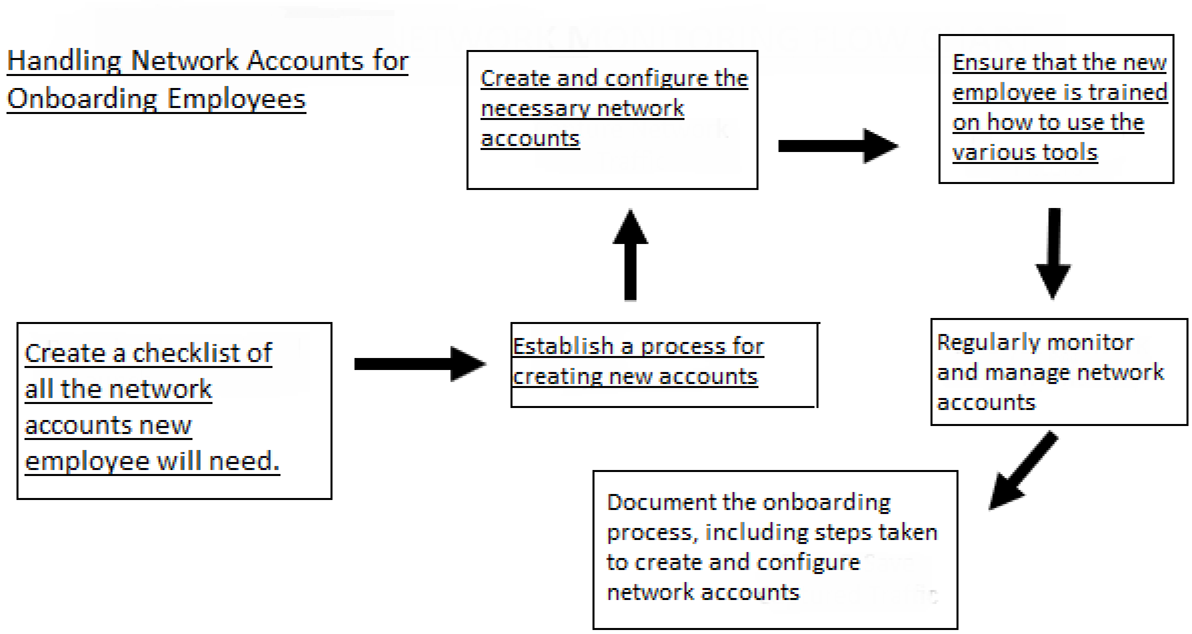
Scope:

This SOP applies to all employees responsible for onboarding new employees and managing network accounts.

Responsibilities:

- The HR team is responsible for collecting the necessary information from the new employee.
- IT Specialist Damian Nowak is responsible for creating and configuring the network accounts and granting access to tools and software.
- The new employee is responsible for attending training sessions and familiarizing themselves with the tools and software they have been granted access to.

Procedure:


Handling Network Accounts for Onboarding Employees
Create a checklist of all the network accounts new employee will need.
Establish a process for creating new accounts
Create and configure the necessary network accounts
Ensure that the new employee is trained on how to use the various tools
Regularly monitor and manage network accounts
Document the onboarding process, including steps taken to create and configure network accounts

-

- Create a checklist of all the network accounts and tools the new employee will need. This should include email, computer login, VPN access, and any other tools or software specific to your organization.
  - Identify all the network accounts and tools that the new employee will need to perform their job effectively. This may include email, computer login, VPN access, and any other tools or software specific to your organization.
  - List each network account and tool on the checklist. Ensure that the list is comprehensive and includes all necessary information such as login credentials, software versions, and account permissions.
  - Determine the access level required for each account and tool. Some accounts may need full access, while others may require restricted access based on the employee's role.
  - Prioritize the checklist based on the importance and urgency of each network account and tool. This will help ensure that the new employee has access to critical tools and software from day one.
  - Review the checklist with the new employee during their onboarding process to ensure that they have a clear understanding of the network accounts and tools they will be using. Make sure to answer any questions they may have and provide instructions on how to access each account and tool.

- Establish a process for creating new accounts and collect all necessary information from the new employee to create their network accounts.

    - Determine who will be responsible for creating new network accounts. This may be an IT team member or an automated account creation tool.
    - Develop a process for creating new accounts that includes the necessary steps and procedures to ensure that accounts are created accurately and securely.
    - Create a form or document that the new employee will fill out with all necessary information to create their network accounts. This may include their full name, job title, department, email address, phone number, and any other information specific to your organization.
    - Collect any additional information required for each specific network account or tool. For example, if the new employee will need VPN access, you may need to collect their IP address or other identifying information.
    - Store the new employee's information securely in a centralized location. This will help ensure that the information is easily accessible and can be used to create all necessary accounts.

- Create and configure the necessary network accounts for the new employee, set up permissions and access levels based on their role, and communicate login information to the new employee.
    - Use the checklist created in the previous step to identify the necessary network accounts for the new employee.
    - Create each network account using the information collected in the previous step. Make sure to use secure passwords and follow any other security protocols specific to your organization.
    - Configure each account to reflect the new employee's role and responsibilities. This may include setting up permissions and access levels based on their job title or department.
    - Test each network account to ensure that it is working properly and that the new employee has the necessary access to perform their job.
    - Once all network accounts have been created and configured, communicate the login information to the new employee. Provide clear instructions on how to access each account and tool, and answer any questions they may have.

- Ensure that the new employee is trained on how to use the various tools and software they have been granted access to.
    - Develop a training plan that outlines the various tools and software the new employee will need to use, and the level of training required for each.
    - Determine the best method of training for each tool or software. This may include one-on-one training sessions, group training sessions, or access to training resources such as videos, manuals, and online tutorials.
    - Schedule training sessions and provide the new employee with any necessary training materials or resources.

- During the training sessions, provide clear instructions on how to use each tool or software, and answer any questions the new employee may have.
- Monitor the new employee's progress and provide additional training or support as needed.
- Ensure that the new employee understands the security protocols and best practices for using each tool or software.
- Provide ongoing training and support as needed to help the new employee succeed in their job.

- Regularly monitor and manage network accounts to ensure that only authorized personnel have access, and document the onboarding process in the employee's personnel file. Additionally, review and update the SOP periodically to ensure that it remains current and effective.
    - Develop a process for regularly monitoring and managing network accounts. This may include conducting periodic security audits, reviewing access logs, and revoking access for employees who no longer require it.
    - Train relevant personnel on how to monitor and manage network accounts, including how to identify and respond to security threats.
    - Regularly review the network accounts of current employees to ensure that they have only the necessary access to perform their job.
    - Document the onboarding process, including steps taken to create and configure network accounts, in the employee's personnel file. This will help ensure that there is a clear record of the employee's access levels and permissions.
    - Review and update the SOP periodically to ensure that it remains current and effective. This may include incorporating new tools or software, updating security protocols, or adjusting processes based on feedback or changes in organizational structure.

Definitions:

- SOP – Standard Operating Procedure

Revision History:

03APR2023 – Uploaded SOP template – Ethan Brock
05APR2023 – Populated Required Info – Jeremy Patton