GILBERT COLLADO

How will network account needs be handled for employees being onboarded?

Purpose:

The purpose of this Standard Operating Procedure (SOP) is to establish a systematic process for creating and managing network accounts for new employees during the onboarding process. This SOP ensures that new employees have timely access to the company's network resources while maintaining security and compliance with company policies.

Scope:

This SOP applies to the IT department of CineTech responsible for creating and managing network accounts for new employees across all departments and locations.

Responsibilities:

- HR Department: Provide necessary employee information to the IT department for account creation.
- IT Department:
    - Create network accounts for new employees.
    - Configure network settings and permissions based on employee roles.
    - Enforce security measures and policies for password management and access control.
    - Provide training and support to new employees regarding network access and usage.

Prerequisites:

- Access to the company's network infrastructure.
- Information provided by HR department including employee name, department, and role.
- Compliance with company security policies and regulations.

Procedure:

1.Receiving Employee Information:

- HR department provides the IT department with employee information including name, department, and role.

2.Network Account Creation:

- IT department creates network accounts for new employees using the provided information.
- Generate unique usernames and passwords for each employee.
- Assign access permissions based on employee roles and responsibilities.

3.Role-based Access Control (RBAC):

- Implement RBAC to ensure that employees have access only to the resources necessary for their job function.
- Assign permissions and privileges according to predefined roles such as Sales, Marketing, R&D, and IT Management.

4.Network Configuration:

- Configure network settings for new employees including IP addresses and VPN access if required.
- Ensure compatibility with the company's central server and other network resources.

5.Security Measures:

- Enforce strong password policies, multi-factor authentication (MFA), and regular password updates.
- Implement network security measures such as firewalls, intrusion detection systems, and encryption protocols.
- Conduct regular security audits to ensure compliance with security policies and regulations.

6.File Share and Collaboration Tools:

- Set up file sharing and collaboration platforms for new employees to facilitate seamless communication and collaboration.
- Apply proper access controls to protect sensitive data and information.

7.Backup Solution:

- Implement a robust backup solution to ensure data integrity and business continuity.
- Regularly backup critical data to both on-site and off-site locations.

8. IT Onboarding Policy:

- Develop and enforce an IT onboarding policy that outlines the procedures and best practices for new employee setup.
- Cover topics such as acceptable use of company resources, data security protocols, and employee training on IT systems.

9.Training and Support:

- Provide comprehensive training to new employees on network access, security protocols, and collaboration tools.
- Offer ongoing support and assistance to address any issues or questions during the onboarding process.

Definitions:

- RBAC: Role-Based Access Control - A method of restricting network access based on the roles of individual users.
- VPN: Virtual Private Network - A secure network connection that allows employees to access the company's network resources remotely.
- MFA: Multi-Factor Authentication - A security process that requires multiple forms of identification to verify a user's identity.

Revision History:

- Version 1.0: Initial SOP created April 15, 2024.