IT Onboarding Policy

Objectives:

This policy outlines the procedures for onboarding new employees into the company's IT environment. It aims to:

- Provide new hires with efficient and seamless access to necessary technology and resources.
- Ensure responsible and secure use of company systems and data.
- Foster a positive first impression and contribute to a smooth transition into the company culture.

Scope:

This policy applies to all new employees, regardless of their position or department. It covers the process from pre-employment to full integration into the company's IT systems.

Procedures:

Pre-Employment:

- The IT department will receive new hire information from HR, including job title, department, and start date.
- Based on the role, the IT department will pre-configure equipment and software licenses.
- New hires will receive an IT Onboarding Guide via email outlining expectations and next steps.

Day 1 - Onboarding:

- Upon arrival, new hires will be welcomed by an IT representative who will assist with device setup and account creation.
- This includes setting up:
    - Network access and email accounts.
    - Office computer and necessary software.
    - Mobile devices, if applicable.
    - Employee access cards or other security credentials.

- New hires will receive initial security training, covering topics like:
    - Password management and best practices.
    - Acceptable use policy for company technology.
    - Data security and reporting procedures.
    - Phishing and malware awareness.

Post-Onboarding:

- Ongoing training will be provided throughout the first week and beyond, depending on the role's specific needs.
- Access to additional resources and support will be available through the IT department's online knowledge base, helpdesk, and internal contact information.
- Periodic audits and security checks will be conducted to ensure compliance with this policy.

Account Creation:

- All accounts will be created by the IT department with strong passwords and multi-factor authentication enabled.
- Account access will be granted based on the principle of least privilege, ensuring users only have access to the resources they need.
- User accounts will be reviewed and disabled upon departure from the company.

Device Setup:

- Company-owned devices will be pre-configured with approved software and security settings.
- Personal devices used for work purposes must comply with the company's acceptable use policy and mobile device management program.

Network Access:

- Access to the company network will be controlled through a firewall and monitored for suspicious activity.
- Use of unauthorized software or hardware on the network is strictly prohibited.
- Wi-Fi access for personal devices will be separate from the corporate network.

Security Training:

- All new hires will undergo mandatory security training, covering topics like:
    - Cybersecurity threats and vulnerabilities.
    - Data privacy and compliance regulations.
    - Incident reporting procedures.
    - Social engineering and phishing awareness.
    - Password security and best practices.

Compliance:

- All employees are responsible for complying with this policy and reporting any potential security vulnerabilities or policy violations.
- Non-compliance may result in disciplinary action, up to and including termination of employment.

Review and Updates:

- This policy will be reviewed and updated periodically to reflect changes in technology, security best practices, and company needs.