Standard Operating Procedure (SOP): Onboarding New Users

Owner: IFC - IT Department
Date Created: 03/27/2025
Version: 2.0

Table of Contents

Introduction

This SOP defines the step-by-step process for onboarding new hires within the organization. The goal is to ensure that new employees have the necessary tools, access, and security measures in place to perform their roles efficiently.

Prerequisites

Before proceeding with the onboarding process, ensure the following are completed:

- **HR Confirmation:** HR has approved the new hire's start date, role, and department.
- **Device Allocation:** A designated workstation (laptop/desktop) is ready.
- **Software & Licensing Requirements:** List of required applications and subscriptions based on role.
- **Access Approvals:** Approval received from HR or management for provisioning access.

Procedure

1. Add User to Microsoft

Step 1: Log in to **Microsoft Entra Admin Center**.

Step 2: Navigate to **Users > Active Users**.

Step 3: Click **"Add User"** and enter the following details:

- First Name, Last Name
- Email Address
- Department and Job Title

Step 4: Assign the necessary **Microsoft 365 licenses** (e.g., Microsoft 365 Business Premium).

Step 5: Set a **temporary password** and enable **mandate password change on first login**.

Step 6: Click **Create**, verify the user is added successfully.

2. Add User to Monday.com

Step 1: Access the **Monday.com platform** using admin credentials.
Step 2: Navigate to the section where **user management** and **permissions** are configured.
Step 3: Initiate the process to **add or invite** the new hire, entering the required information.
Step 4: Link the user to the **necessary areas** of the platform relevant to their role.
Step 5: Adjust settings to ensure **appropriate access levels**.
Step 6: Finalize the process and confirm successful integration.

3. Setup Workstation

Step 1: Complete Initial Windows Setup

- Turn on the device.
- Select the **preferred language, region, and keyboard layout**.
- Connect to a **Wi-Fi network** or use an **Ethernet cable** for internet access.
- Click **Next** to proceed.
- When prompted, select **Set up for work or school**.
- Sign in with the **organization's Microsoft 365 admin account** to start the configuration.

Step 2: Install Windows Updates

- Go to **Settings > Update & Security > Windows Update**.
- Click **Check for updates** and install all available updates.
- Restart the device as needed.

Step 3: Configure Device Policies via Intune

- Enroll the device into **Microsoft Intune** using the organization's credentials.
- Ensure that the device is compliant with **security and endpoint policies**.

Step 4: Install Required Software and Tools

- Download and install the **Microsoft Office Suite** from the organization's portal.
- Install **Microsoft Teams**, security software, and other job-specific applications.
- Configure settings for **VPN, antivirus, and endpoint protection**.

Step 5: Add User Profile

- Go to **Settings > Accounts > Other Users**.
- Click **Add a work or school account**.
- Enter the new hire's **Microsoft 365 credentials**.
- Log in using the **temporary password** and prompt the user to set a new password.

4. Add Device to Microsoft Intune & Update Inventory

Step 1: Enroll the workstation into Microsoft Intune:

- Open **Microsoft Endpoint Manager Admin Center**.
- Navigate to **Devices > Enroll Devices**.
- Select **Windows Enrollment** and complete the registration process.

Step 2: Assign the device to the **new hire's user profile**.

Step 3: Apply **security policies, compliance settings, and remote management settings**.

Step 4: Verify the **Remote Monitoring & Management (RRM) configuration**.

Step 5: Update **hardware inventory** by logging device details:

- Device Name
- Serial Number
- Asset Tag
- Assigned User

5. Provide Adobe License (As Needed)

Step 1: Log in to **Adobe Admin Console**.

Step 2: Navigate to **Users > Assign Users**.

Step 3: Enter the **new hire's email address**.

Step 4: Assign the appropriate **Adobe Creative Cloud or Acrobat license**.

Step 5: Save changes and confirm access.

6. Provide Access to Required Software

Step 1: Identify all **job-specific applications** the new hire needs.

Step 2: Assign access via **Microsoft Entra ID.**

Step 3: Add the user to the appropriate **security groups and application groups**.

Step 4: Install the **licensed software** as required.

Step 5: Conduct an **access test** to ensure all necessary tools work.

7. Verification & Handover (Joining Day Tasks)

Step 1: Assist the new hire with first login:

- Guide them through signing into their workstation and Microsoft account.

Step 2: Ensure the user changes their password upon first login:

- Prompt them to set a new, strong password.

Step 3: Set up Multi-Factor Authentication (MFA):

- Instruct the new hire to install **Microsoft Authenticator** (mandatory).
- Guide them through **MFA registration** using the Microsoft Authenticator app.

Step 4: Add the new hire to required Microsoft Teams channels:

- Log in to **Microsoft Teams**
- Locate their department's **Teams and Channels**.
- Add them to relevant channels.

Step 5: Conduct an access verification check:

- Confirm that the new hire has access to email, OneDrive, Teams, and other tools.
- Assist with any initial technical issues.

8. Biometric Setup for Door Access

Step 1: Register the New Hire in the ZKT Biometric System

- Log in to the **ZKT Access Control System** using the administrator credentials.
- Navigate to **User Management > Add New User**.
- Enter the required details:
  - Employee Name
  - Employee ID
  - Department
  - Job Title

Step 2: Enroll Biometric Data

- Select **Fingerprint Registration**
- Instruct the new hire to place their finger on the **ZKT biometric scanner** multiples times until enrollment is successful.
- Save the data and synchronize with the access control system.

Step 3: Test Biometric Access

- Have the new hire scan their fingerprint at the designated access point.
- Verify that the system grants entry without issues.
- Troubleshoot and re-register the biometric data if access fails.

Conclusion

This SOP ensures a smooth and secure onboarding process for new hires, providing them with the necessary tools, access, and security configurations to perform their roles effectively. By following these structured steps, IT can standardize onboarding, minimize delays, and maintain compliance with security policies. Regular reviews and updates to this SOP will help adapt to evolving technology and organizational needs.