SNOWBE ONLINE

Procedure # NU-01

Creating New User Account

Daphnie Bruno

Procedure # NU-01 Version # 1.3

November 13, 2024

Table of Contents

Purpose

This procedure outlines the steps for creating user accounts on SnowBe Online Systems. The purpose of this procedure is to detail the steps involved in establishing new user accounts for both internal employees and external customers. It ensures a consistent account creation process throughout the organization.

Scope

This procedure is relevant for internal users, including new employees, contractors, vendors who need access to SnowBe Online's systems, and external users, who are customers creating accounts on SnowBe's website for purchases and services. These accounts ensure accountability, which is essential for any computer security program. Therefore, creating, managing, and monitoring all computer accounts are vital to an overall security strategy.

Definitions

Account

Any combination of a User ID (sometime referred to as a username) and a password that grants an authorized user access to a computer, an application, the network, or any other information or technology resource.

Active Directory (AD)

A directory service used for account management and authentication of internal user accounts.

Authorization

The process of obtaining approval for account creation. Also could be used to refer to when user obtains permission.

Multi-Factor Authentication (MFA)

A security system that requires more than one method of authentication from independent categories of credentials to verify the user’s identity.

Permission

Is the organizational (Org) unit that is assigned to the Role that will allow the user access to a specific or multiple Org units.

Role

This describes the function a user can perform on the system, e.g. view reports, capture data, create user accounts for specific module on the information system.

Security Administrator

The person charged with monitoring and implementing security controls and procedures for a system. Whereas SnowBe Online may have one Information Security Officer, technical management may designate several security administrators.

System Administrator

The person responsible for the effective operation and maintenance of information systems, including implementation of standard procedures and controls to enforce an organization's security policy.

Verification Link

An email generated link that a customer will receive to confirm their account during creation.

Roles & Responsibilities

Chief Information Security Officer (CISO)

- Oversee the development and implementation of the new account creation procedure.
- Ensure the procedure aligns with overall information security strategy.
- Approve the final procedure document.
- Periodically review and update the procedure as needed.

Compliance Officer

- Ensure the new account creation procedure complies with relevant regulations and industry standards.
- Review the procedure for adherence to compliance requirements.
- Provide input on necessary controls and documentation for compliance purposes.

Customer Service

- Provide accurate information for account creation.
- Responsible for assisting customers with any issues during the account creation process.
- Resolve customer inquiries related to registration and access.

Employees

- Follow the established procedures for requesting new accounts.
- Provide accurate information for account creation.
- Complete any required training on account security and usage.
- Adhere to the procedure guidelines for account management and security.

Human Resources

- Initiate the account creation process for new hires.
- Provide necessary employee information to IT for account setup.
- Notify IT of employee status changes (e.g., transfers, terminations) that affect account management.
- Ensure new employees complete required security awareness training.

IT Security Manager

- Develop and maintain the technical aspects of the account creation procedure.
- Implement security controls and monitoring for new accounts.
- Regularly audit account creation procedure for compliance with the procedure.
- Provide guidance on security best practices for account management.

IT Security Officer

- Assist in developing security requirements for new accounts.
- Monitor account creation activities for potential security risks.
- Investigate and report any security incidents related to account creation.
- Provide security recommendations for procedure improvements.

IT Staff

- Execute the technical aspects of account creation.
- Set up accounts with appropriate access levels and permissions.
- Implement and maintain account management systems.
- Provide technical support for account-related issues.

Management

- Approve the new account creation procedure.
- Allocate necessary resources for procedure implementation.
- Support enforcement of the procedure across the organization.
- Review and approve any exceptions to the procedure.

Third-Party Vendors

- Comply with the organization's account creation procedure when applicable.
- Provide necessary information for account creation if given access to internal systems.
- Adhere to security requirements specified in the procedure and contracts.
- Report any security concerns or incidents related to provided accounts.

User

- External users (customers) are responsible for verifying their email and securing their account credentials.

Procedure

Below you will find a step-by-step procedure for creating a new user account in Windows 2020 using Active Directory with multi-factor authentication (MFA) and a new user procedure to log into www.snowbeonline.com and register for the first time to create a new user account.

NU-1.1 Getting started

By following these steps, you'll be able to turn on your windows computer, log in, open your internet browser, and navigate to a website.

Step 1 Turning on Your Windows Computer:

- Locate the power button on your computer:
    - *For desktop PCs*: Look for the power button on the front or top of the computer case. It's usually in the middle center or top-right corner.
    - *For laptops:* The power button is typically above the keyboard on the left, center, or right side. Sometimes it's on the right hinge of the screen.
- Press the power button once. If nothing happens, press and hold it for about 3-5 seconds.
- If the computer doesn't turn on, ensure its properly plugged in:
    - For desktop PCs: Check that the power cable is securely connected to both the computer and the wall outlet
    - For laptops: Make sure the battery is charged or connect the power adapter and wait 10-30 minutes before trying again
- Wait for the computer to boot up and display the Windows login screen.

Step 2 Logging into Windows:

- Click on your user account icon.
- Enter your password or PIN if prompted.
- Press Enter or click the arrow button to log in.

Step 3 Accessing Your Internet Browser:

- Once the Windows desktop appears, locate your preferred internet browser icon. Common browsers include:
    - Microsoft Edge (blue 'e' icon)
    - Google Chrome (circular icon with red, yellow, green, and blue colors)
    - Mozilla Firefox (circular orange fox icon)
- Double-click the browser icon to open it.
- Wait for the browser to load. Your homepage should appear.

Step 4 Navigating to a Specific Website:

- Click on the address bar at the top of the browser window.
- Type in the web address www.intranet.snowbeonline.com
- Press Enter on your keyboard.
- Wait for the website to load.

NU-1.2 Internal User Account Creation (Employees, Vendors, Contractors)

By following these steps, both IT and the new user can ensure a smooth and secure account creation:

Step 1 Requesting a New User Account:

- Locate and Open your SnowBe Online's IT service portal or ticketing system on www.intranet.snowbeonline.com home page.
- Click on "New Request" or "Submit Ticket."
- Select "New User Account" from the list of available request types.

Step 2 Fill out the form with the following information:

- New user's full name
- Desired username (if applicable)
- Job title
- Department
- Manager's name
- Start date
- Required access levels or group memberships
- Active telephone number
- Submit the request.

Step 3 IT Processes the Request:

- IT receives the new user account request.
- The IT team reviews the request for completeness and accuracy.
- IT seeks approval from the user's manager signed by department head.
- Once approved, IT proceeds with account creation.

Step 4 IT Creates the Account in Active Directory:

- IT administrator logs into the Domain Controller.
- Opens "Active Directory Users and Computers."
- Navigates to the appropriate Organizational Unit (OU) for the new user.
- Right-clicks on the OU and selects "New" > "User."
- Enters the user's information:
  - First name, last name, and full name
  - User logon name (username)
  - Password (meeting complexity requirements)
  - Sets account options:
  - Selects "User must change password at next logon"
  - Configures any other required settings
- Adds the user to appropriate security groups based on their role.

Step 5 Setting Up Multi-Factor Authentication (MFA):

- IT administrator logs into the Azure AD admin center.
- Navigates to "Users" > "All users."
- Selects the newly created user account.
- Clicks on "Authentication methods."
- Enables MFA for the user.
- Configures MFA settings as per company policy.

Step 6 User Notification:

- IT generates an email to the new user containing:
    - Their username
    - Temporary password
    - Instructions for initial login
    - Link to MFA setup guide
- IT sends a separate email to the user's manager with the temporary password.

Step 7 Initial User Login:

- User receives the account creation email.
- User logs into their computer using the provided username and temporary password.
- Windows prompts the user to change their password.
- User enters a new password meeting the company's complexity requirements.

Step 8 MFA Setup:

- User is directed to the MFA setup page on first login.
- User chooses their preferred MFA method (e.g., mobile app, SMS, phone call).
- If using a mobile app:
    - User downloads the authenticator app on their smartphone.
    - User scans the QR code displayed on the MFA setup page.
    - User enters the code generated by the app to complete setup.
- If using SMS or phone call:
    - User enters their phone number.
    - User receives and enters the verification code.

Step 9 Access Verification by IT:

- IT administrator checks the user's account in Active Directory to ensure:
- Account is active
- Correct group memberships are applied
- IT verifies MFA is enabled and set up correctly in Azure AD.
- IT tests the user's access to required resources:
- Attempts to log in to key applications
- Checks file share access
- Verifies email functionality
- IT documents the verification process and results.

Step 10 Final Steps

- IT sends a confirmation email to the user and their manager stating the account is fully set up and verified.
- IT closes the original ticket in the ticketing system.
- IT updates any relevant documentation or user lists.

NU-2.1 External User Account Creation (Customers)

The steps below will walk the customer through creating their online account.

Step 1 Creating a New User Account on www.snowbeonline.com:

- Accessing the Website
- Turn on your computer and wait for it to fully start up.
- Locate and click on your preferred internet browser icon (e.g., Chrome, Firefox, Edge) on your desktop or taskbar.
- Once the browser opens, look for the address bar at the top of the window.
- Click on the address bar to select any existing text.
- Type "www.snowbeonline.com" into the address bar.
- Press the Enter key on your keyboard.

Step 2 Navigating to the Registration Page:

- Wait for the Snow Online website to load completely.
- Look for a "Register" or "Sign Up" button, typically located in the top right corner of the page.
- Click on the "Register" or "Sign Up" button.
- Filling Out the Registration Form
- On the registration page, you will see a form with several fields to fill out:
- Start with the "Personal Information" section:
    - Enter your first name
    - Enter your last name
    - Type in your email address
    - Re-enter your email address to confirm it
- Move to the "Account Information" section:
    - Create a username (follow any specific requirements listed)
    - Create a password (ensure it meets the stated security requirements)
    - Re-enter your password to confirm it
- Fill out any additional required fields, which may include:
    - Date of birth
    - Phone number
    - Address
- Read through the terms of service and privacy policy.
- Check the box to agree to the terms and conditions.

Step 3 Completing the Registration:

- Look for a "Create Account" or "Register" button at the bottom of the form.
- Click the "Create Account" or "Register" button.
- Wait for the system to process your information.
- Verifying Your Account
- Check your email inbox for a message from Snow Online.
    - If you don't see it, check your spam or junk folder.
- Open the email from Snow Online.
- Look for a verification link or button in the email.
- Click on the verification link or button.

Step 4 Logging in for the First Time:

- You will be redirected to the login page.
- Enter the username you created during registration.
- Enter the password you created during registration.
- Click the "Log In" button.

Step 5 Completing your Profile:

- You may be prompted to complete your profile with additional information.
- Fill out any required fields.
- Click "Save" or "Update Profile" when finished.

NU-3.1 Warnings and Exceptions

Internal Accounts

- If account setup is not completed within 48 hours, the department head must escalate the issue to IT management.

External Accounts

- Customer account creation requests will be automatically canceled if email verification is not completed within 7 days.

NU-4.1 Security Warning

- All users are strictly prohibited from sharing passwords. Adherence to the company's password security guidelines is mandatory for all account holders.
- This procedure is subject to regular review and may be updated to reflect changes in technology, business practices, or regulatory requirements.

Exceptions/Exemptions

Exceptions to this Security Plan are only permissible in rare situations where strict adherence would significantly disrupt business operations.

- Any request for an exception must be made in writing to the IT Security Manager.
- The IT Security Manager will evaluate it in collaboration with pertinent stakeholders.
- If granted, the exception will be in place until the policy changes or the person's employment status changes.
- The IT Security Manager and the Risk Management team will perform a detailed risk assessment and put suitable compensation controls in place to reduce potential risks during the exception period.
- The approval of exceptions will depend on these mitigating measures.

Enforcement

Violations of this IT Security Plan will result in disciplinary actions, which may include, but are not limited to, verbal or written warnings, suspension, termination of employment, or legal action, depending on the severity of the violation.

- 1st violation, verbal coaching.
- 2nd violation, written coaching.
- 3rd violation, associate retraining.
- 4th violation, suspension.
- 5th violation, termination.

Regular audits and monitoring will be conducted to ensure compliance, and employees are encouraged to report any suspected security incidents or policy breaches to the IT Security team immediately. IT audits will be conducted monthly at discretion of the IT manager. The senior IT Manager will summarize the audit findings monthly and present it to the CISO.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	12-Nov-24	Daphnie Bruno		Created rough draft of procedure
1.2	13-Nov-24	Daphnie Bruno		Created step by step guide for internal and external users
1.3	14-Nov-24	Daphnie Bruno		Fixed Table of content Finalized document

Citations

- Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com Used to correct grammar errors and spelling errors.
- SOP – User Accounts
- PDF – Ideal Clinic Monitoring System
- PDF – Account Creation Procedures
- PDF – Colorado Department of Education
- User Account creation and management
- ScienceLogic
- Oracle docs – Creating users
- IBM – Creating User Accounts
- Cal Poly
- PurpleSec
- ComputerHope
- Creating new user
- HP Tech Takes
- Harvard College Account Creation