

SNOWBE ONLINE Policy# 25

Create a New Account Procedure

Your name: Tyrall Waller

Group 6 Section 01

Draft - Version # 3.1

DATE: 3/23/25

Table of Contents

PURPOSE **2**

SCOPE **2**

DEFINITIONS **2**

ROLES & RESPONSIBILITIES **2**

POLICY & PROCEDURES **3**

EXCEPTIONS/EXEMPTIONS **6**

ENFORCEMENT **7**

VERSION HISTORY TABLE **9**

CITATIONS **10**

Purpose

The purpose of this procedure is to provide the necessary steps to create a new account for SnowBe customers. The procedures provided have been created to ensure customer information is properly collected, stored and protected by SnowBe employed personnel and kept within the standards for legal and regulatory compliance. The number one priority is to ensure customer data, account management and the business to client relationship delivers a secure and smooth process with all SnowBe business operations.

Scope

The Create a New Account procedure applies to all system users and employees who create, access, process, and handle informational data within the SnowBe business of operations. These procedures focus on new account creation, collection, storage and processing of customer data, credit card payment and customer transactions and the handling of account data within the SnowBe website.

The established procedures for the enforcement of creating a new account provide guidelines that ensure that all SnowBe personnel and all authorized access users adhere to the directed standards and utilization of resources.

Definitions

Sensitive data: Personal information which includes names, addresses, phone numbers, email addresses, credit card information and purchase history.

Encryption: The process of converting plaintext into ciphertext using a cryptographic algorithm and a key, making the information unreadable to anyone who does not have the appropriate key to decrypt the message.

Multi-factor Authentication: Multi-step process that requires users to enter More information as verification of identity to gain access to an account.

Roles & Responsibilities

Employees:

Must read and understand the procedure that has been put in place.

Obligated to take ownership and responsibility by following established protocols in order to properly perform and demonstrate compliance with the guided process for creating new account protection in a secure manner.

Required to adhere to the directed security practice for login credentials, strong password and proper disposal of sensitive data guidelines.

Required to report unusual activity and possible and identified data breaches, and security incidents to the authorities and higher management.

Must comply with all relevant laws, regulations and internal policies and procedures related to creating a new account access.

Information Technology Team:

Maintain the infrastructure, and implement all systems, firewalls and encryption protection.

Manage and audit new account access for accuracy of new account.

Audit system for access enforcement compliance within daily activity.

Have on-hand procedures for incident response for all incidents.

Security Team:

Provide scheduled security training to all hands.

Create, revise, maintain and cancel all policies and procedures.

Investigate and report all security and access incidents to higher authority with an after action report and follow-up action to resolve the related incident.

Monitor all activity to ensure all compliance regulations are being followed.

Identify, gather and analyze threat intel for possible risk or vulnerability.

Policy

The implementation of this procedure enables employees and customers the ability to create a new account. Customer personal and financial data is processed and stored within compliance of the Payment Card Industry Data Security Standard as well as being protected by encryption. Each customer has access to make necessary adjustments and changes to their account for business interaction and transactional purposes. All activity is monitored and audited for secure processing, and inactive use. The privacy policy, terms and conditions that ensure customer data is protected and not shared without

consent must receive consent by each customer.

Procedures

Step 1: Customer Information Collection

Personal Information

Collect the following details from the customer:

Full Name (First and Last)

Email Address

Phone Number

Mailing Address (Billing and Shipping)

Date of Birth (if applicable)

Ensure that all personal data is collected securely through HTTPS connections.

Account Information

Allow the customer to choose a username for their account.

Require a strong password (minimum of 8 characters, including at least one number and one special character).

Optionally, provide security questions and answers for account recovery.

Payment Information

Request payment information such as:

Credit Card Number (processed securely via PCI-DSS compliant gateway)

Billing Address (if different from the mailing address)

Ensure that credit card data is tokenized or encrypted.

Step 2: Secure Data Storage

Data Encryption

All customer data, including personal, payment, and transaction data, should be encrypted during transit (using SSL/TLS) and at rest (using strong encryption algorithms).

Tokenization

Payment information should be tokenized and stored in a separate, PCI-DSS compliant database. Direct storage of raw credit card numbers is prohibited.

Step 3: Multi-Factor Authentication (MFA)

Authentication Requirement

All customer accounts should be protected by Multi-Factor Authentication (MFA) .

Customers must authenticate using at least two factors (e.g., password and email/SMS verification code) before performing sensitive actions like changing payment methods.

Password Recovery

Allow customers to securely reset passwords using a reliable recovery method (email, SMS, or security questions).

Send password reset links through time-limited emails or SMS messages.

Step 4: Terms and Conditions / Privacy Policy Agreement

Customer Agreement

Before finalizing account creation, customers must review and accept:

Terms and Conditions

Privacy Policy

Payment and Refund Policy (if applicable)

This consent must be confirmed by the customer checking the opt-in box.

Step 5: Account Verification

Email Verification

Send a verification link to the customer's email address after registration.

The customer must click the link to verify their email address before they can access the full features of their account.

Step 6: Confirmation and Welcome Email

Welcome Message

Upon successful account creation and email verification, send a welcome email that includes:

Customer's username

A summary of account settings (email, billing/shipping address)

Instructions on how to access the customer portal

Information about the first order or loyalty program (if applicable).

Step 7: Data Retention and Archiving

Login Audit Logs

All login attempts (successful and failed) must be logged for security and auditing purposes.

These logs should be stored for at least **90 days** and archived securely to a cloud storage system for long-term retention.

Customer Data Retention

Retain customer data as required by business needs and compliance laws.

Customer purchase history and associated data should be archived securely and deleted in compliance with applicable data retention regulations.

Step 8: Mobile Device Security

Device Approval

Mobile Device Management (MDM) solutions should be implemented to approve and control which mobile devices can access SnowBe's Online internal data. Devices not enrolled in the MDM system should be restricted from accessing customer accounts or any internal data.

Encryption and Remote Wipe

All mobile devices must have encryption enabled.

In case of device theft or loss, enable remote wipe to prevent unauthorized access.

Step 9: PCI Compliance

PCI-DSS Requirements

Ensure that all systems processing, storing, or transmitting payment data are fully compliant with PCI-DSS standards.

Implement controls such as:

Encryption of cardholder data.

Regular vulnerability scans and penetration testing.

Secure access controls to sensitive systems and data.

Step 10: Ongoing Security Monitoring

Continuous Monitoring

Continuously monitor for security threats, anomalies, or unauthorized access.

Implement automated systems for real-time alerts when any unusual activity is detected, especially related to customer accounts or payment data.

Regular Audits

Conduct periodic audits of customer data storage, access control, and security logs to ensure compliance with internal policies and industry regulations.

Exceptions/Exemptions

To ensure flexibility in security implementation while maintaining strong controls, the following exception/exemption policy applies:

1. Request Process:

a. Any request for an exception/exemption must be submitted in writing to the IT Security Manager.

b. The request must outline the reason, the systems affected, and the duration required.

2. Justification: The request must provide a valid business or operational reason that necessitates an exception.

3. Approved Authority: Approval must be granted by both the IT Manager and IT Director.

4. Duration:

a. Exceptions/exemptions will be granted for a limited period,

subject to review every 6 months.

b. If an extension is required, a new request must be submitted along with the previous action provided.

Enforcement

A discharge by an employer of an individual for violation of an employer rule is for misconduct connected with the work if the rule is reasonable, the individual knew or should have known the rule, and the violation is willful or wanton, material, and substantially injures or tends to injure the employer's interests.

If the individual has previously violated a minor employer rule or has previously violated the same or a similar employer rule with the knowledge of the employer, a discharge is for misconduct connected with the work if the violation substantially injures or tends to injure the employer's interests and has been preceded by prior warnings or reprimands for previous violations, or if the individual's course of conduct as a whole demonstrates a substantial disregard of the employer's interests following prior warnings or reprimands for violations of other employer rules.

Thus, a violation of an employer rule is not, by itself, misconduct. It would be misconduct if all of the following conditions are met:

The rule is reasonable.

The claimant knew or should have known the rule.

The violation is willful and wanton.

NOTE: Violation of a reasonable employer rule is not willful if the claimant has shown good cause for violating the rule.

The violation is material.

The violation substantially injures or tends to injure the employer's interests.

The employer has warned or reprimanded the claimant for previous violations of the same or similar employer rules.

Reasonable Rule

It is the employer's right generally to establish such rules for his or her employees as, in the employer's opinion, are necessary for the proper conduct of his or her business. Violation of an employer rule regarding the performance of the work will generally be a violation of a reasonable rule.

Knowledge of Rule

To be known, a rule must have been disseminated generally to all employees or made known to the claimant individually, either orally or in writing.

If a claimant has been given a written copy of employer rules (as in an employee handbook), his or her failure to read the rules would not render the discharge for reasons other than misconduct. If the claimant was never informed of the existence of the employer rule, the discharge for violating the rule would generally not be for misconduct.

Some employer rules, however, do not need to be transmitted to the employee but are implied or are known rules in the occupation or industry. For example, there does not need to be a written employer rule against stealing of employer property or a formal employer rule that an employee in a bank does not drink on the job.

Violation is Willful

If a claimant has good cause for his or her violation of a rule, or if the violation is due to mere inefficiency, unsatisfactory conduct, failure in good performance as the result of inability or incapacity, inadvertence or ordinary negligence in isolated instances, or good faith errors in judgment or discretion, then there is no misconduct. Under such circumstances, the violation of the rule would not be a willful, deliberate, or flagrant violation.

Materiality of Rule Violation

Violation of an employer rule is material when the employer's operations are interfered with.

Substantial Injury to Employer's Interest

From the definition of a "reasonable employer rule," it follows that any violation of a reasonable rule will injure or tend to injure the employer's interests. However, there is no misconduct unless the injury or tendency to injure is substantial.

Warnings and Reprimands

Some employer rules are such that their first violations would be misconduct, for example, rules prohibiting fighting or drinking on the job. Warnings and reprimands need not be considered for this kind of violations.

However, if the claimant has broken an employer rule which, although reasonable, is of comparatively slight significance, the claimant should be entitled to a warning or reprimand so that he or she would have the opportunity of mending ways before he or she was discharged. Therefore, if the employer has a rule about tardiness, or overstaying coffee-breaks, or any of the more minor conditions of employment, to constitute misconduct the employer would need to show that the claimant persisted in violating the rule despite warnings and/or reprimands.

What if the warnings or reprimands were not for the same type violations as the one which occasioned the claimant's discharge? Even so, the discharge would be for misconduct if the claimant's conduct, viewed in its entirety, evinced a deliberate disregard of the employer's interests. For example, a claimant may have been warned several times over a period of two or three months because of such violations as arguing with coworkers, wandering away from the workstation to engage in conversations, and failure to follow instructions. If, shortly after the last warning, the claimant violated an employer rule relative to tardiness by appearing at work 20 minutes late without good cause and was thereupon discharged, the discharge would be for misconduct.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
3.1	3/23/25	Tyrall Waller	Tyrall Waller	Create a New Account Procedure

Create a New Account Procedure – V 3.1
Status: ✖ Working Draft ☐ Approved ☐ Adopted
Document owner: Tyrall Waller
DATE 3/23/25

Citations

Creating an Amazon Account

(Centre for Equitable Library Access, 2024)

<https://celalibrary.ca/EDOP-Creating-an-Amazon-Account>

How to sign up for Netflix

(Netflix, Unknown)

<https://help.netflix.com/en/node/112419>