SNOWBE ONLINE SECURITY PLAN

Table of Contents

Section 1: Introduction

The purpose of this Security Plan is to create effective administrative, technical, and physical safeguards to protect our customers' non-public personal information. It will also establish a comprehensive framework to protect SnowBe Online's assets, including its data, infrastructure, and business processes, from potential security threats and vulnerabilities. The plan will evaluate our electronic and physical methods of accessing, collecting, storing, using, transmitting, protecting, and disposing of our customers' non-public personal information.

Section 2: Scope

The scope of this Security Plan covers all aspects of SnowBe Online's technical infrastructure, operations, and data management practices. This plan applies to all the following groups and individuals and company assets: employees, IT and security teams, management and executives, third-party vendors and Contractors, storefront staff, end-users with access to company systems, and Auditors and Compliance Officials. The assets are the website itself, company laptops, servers, credit card terminals (storefront), and hardware and software components.

Section 3: Definitions

Access Control:

The process of restricting and granting access to systems, data, and resources based on defined policies and roles.

Account Credentials:

A combination of a username and password or other authentication mechanism used to gain access to a system or resource.

Account Deactivation:

The process of disabling a user account to prevent further access to systems and resources.

Account Lifecycle: The phases of account management, including creation, modification, and termination.

Audit Logs:

Records of activities performed within an information system used for monitoring and compliance.

Account Lockout:

A security feature that disables a user account temporarily after a specified number of consecutive failed login attempts.

Authentication:

The process of verifying the identity of a user, system, or entity attempting to access a resource.

Backup/Disaster Recovery:

Procedures to ensure data integrity and availability in the event of system failure or a security incident.

Brute-Force Attack:

A method of attempting to gain access to accounts by systematically trying every possible password combination.

Change Control: Change Control is a systematic approach to managing all changes to company IT Resources. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted, and that resources are used efficiently.

Cloud-Based Systems:

Platforms or applications hosted on external servers that can be accessed via the internet, such as AWS.

Compliance:

Adherence to regulatory and security standards, such as PCI DSS and NIST 800-53, ensuring the organization meets legal and ethical requirements.

Complex Password:

A password that meets specific criteria for length, character diversity (e.g., uppercase, lowercase, numbers, symbols), and avoids common words or patterns.

Credential Compromise:

The unauthorized disclosure or theft of login credentials (e.g., username and password).

Data Breach:

An incident in which sensitive, confidential, or protected data is accessed or disclosed without authorization.

Data Classification:

The process of categorizing data based on its sensitivity and criticality to the organization.

Data Encryption:

The use of cryptographic methods to secure data both at rest and in transit, ensuring confidentiality and integrity.

Desktops: for this policy, includes but is not limited to laptops, notebooks, or any “personal computer” that can be accessed remotely.

End Users (Employees):

Individuals responsible for using company systems securely and adhering to security policies.

Exceptions:

Situations where deviations from the policy are permitted under specific conditions and approvals.

Firewall:

A network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Hashing:

A cryptographic process used to convert passwords into a fixed-length, irreversible string of characters for secure storage.

Inactive Accounts:

User accounts that have not been accessed for a predefined period and are subject to review or deactivation.

Inactive Accounts: include computing, networking, communications, application, telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

IT Resources:

Include computing, networking, communications, application, telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and related materials and services.

Incident Response Team:

A group responsible for responding to security incidents, minimizing potential damage, and conducting post incident analysis.

Least Privilege:

A security principle granting users the minimum level of access necessary to perform their job duties.

Malware Protection:

Policies and tools designed to detect, prevent, and respond to malicious software threats.

Multi-Factor Authentication (MFA):

An authentication method requiring two or more verification factors to gain access to systems or resources.

Network Security:

Policies and technologies designed to protect the integrity, confidentiality, and availability of a network and its data.

Network Segmentation:
The practice of dividing a network into smaller segments to enhance security and limit unauthorized access.

NIST 800-53:
A framework provided by the National Institute of Standards and Technology outlining security and privacy controls for organizations.

Payment Card Industry Data Security Standard (PCI DSS):
A set of security standards designed to ensure that companies process, store, and transmit credit card information securely.

Physical Security:
Measures designed to prevent unauthorized physical access to systems, buildings, and data storage facilities.

Privileged Accounts:
Accounts with elevated permissions, typically used by system administrators for critical operations.

Public-Facing Applications:
Applications or systems that are accessible by external users or customers, such as the WordPress shopping cart.

Remote Access:
The ability to access an organization’s systems and data from a location outside its physical premises.

Role-Based Access Control (RBAC):
A security model where access permissions are assigned based on the user’s role within the organization.

Service Accounts:
Non-human accounts used by applications or systems to perform automated processes or services.

System Administrators:
Personnel responsible for the secure operation and maintenance of company systems and servers.

Security Awareness Training:
Programs designed to educate employees about security policies, risks, and best practices.

Sensitive Data:
Information that, if disclosed, could cause harm to the organization or its customers.

Third-Party Vendors:
External entities providing services or systems, responsible for adhering to SnowBe Online’s security policies and regulations.

User Accounts:
Individual accounts assigned to users for accessing systems and data, typically requiring credentials such as a username and password.

Virtual Private Network (VPN):
A secure network connection that encrypts data, allowing remote access to internal systems while ensuring confidentiality.

Wireless Access Points:
Is a networking device that allows wireless devices to connect to a wired network.

Wireless Systems:
Networks and devices that use wireless communication technologies to connect to SnowBe Online’s resources.

Section 4: Roles & Responsibilities

Audit Team:
The Audit Team ensures the effectiveness of security controls through regular evaluations. They review logs, processes, and reports, identifying areas for improvement and recommending changes to ensure compliance with SnowBe Online’s policies and regulatory standards.

Change Control Board (CCB):
A group of stakeholders who review, approve, or reject change requests based on their impact and alignment with business objectives. Includes representatives from IT, operations, and management.

Change Requester:
The individual or team proposing the change. Responsible for documenting the proposed change, providing a business justification, and testing the change in non-production environments.

Chief Information Security Officer (CISO) OR Security Lead:

The CISO or Security lead is responsible for establishing and overseeing SnowBe Online's security strategy, ensuring it aligns with business objectives and regulatory requirements. This role involves conducting risk assessments, developing mitigation strategies, approving security policies, and supervising their implementation.

Compliance Officer:

The Compliance Officer ensures that SnowBe Online follows all relevant regulatory standards, including PCI DSS and NIST 800-53. This role involves managing audit preparations, documenting compliance activities, and working with other departments to implement required controls, ensuring the company remains compliant with all applicable laws and standards.

End Users (Employees): All employees are responsible for complying with SnowBe Online's security policies and using company systems in a secure and responsible manner. This includes participating in regular security awareness training, safeguarding credentials, and reporting phishing attempts or suspicious activities. Remote employees are required to use secure methods, such as VPNs, to access internal company systems.

Executive Leadership:

Executive leadership is responsible for providing all necessary resources. They promote adherence to security policies across the organization and approve any significant changes to security practices or business processes.

Incident Response Team:

The Incident Response Team is tasked with handling security incidents and minimizing potential damage to the company. They investigate root causes, document findings, and update the incident response plan as needed. The team also conducts regular exercises to ensure readiness for future incidents.

IT Manager/Infrastructure Team: The IT Manager is responsible for maintaining and securing the company's IT infrastructure, which includes servers, desktops, laptops, and network devices. This involves ensuring all devices are updated with the latest hardware and software, securing physical assets like on-premises servers, and overseeing the implementation of disaster recovery processes.

Legal and Compliance Team:

Ensures account creation procedures comply with legal and regulatory requirements.

Reviews privileged account requests and oversees any exceptions to standard processes.

Managers (Department Heads):

Access Request Approval: Approve access requests based on employee job roles and business needs

Network Administrators:

The Network Administrators secure and manage all network devices, including firewalls, routers, and switches. They ensure the network infrastructure is updated, segmented appropriately, and monitored for potential threats. They also establish secure remote access solutions, such as VPNs, and maintain activity logs for auditing and forensic purposes.

Security Analyst:

The Security Analyst plays a vital role in identifying and mitigating security risks. This involves conducting vulnerability scans, penetration tests, and regular risk assessments. The Security Analyst monitors the organization's systems for potential threats, investigates incidents, and provides actionable recommendations to improve SnowBe Online's security posture.

System Administrators:

System Administrators are responsible for the secure operation of SnowBe Online's on-premises and cloud based servers (AWS). Their duties include implementing access controls based on the principle of least privilege, deploying and managing antivirus solutions, and maintaining critical systems such as the WordPress shopping cart to ensure reliable and secure operations.

Retail Staff:

Retail staff are responsible for securely handling customer credit card transactions at physical storefronts. This includes following company policies for payment terminal use and ensuring customer data is processed securely. They are also expected to report any suspicious activities or system anomalies to the appropriate teams.

Requester:

Submits a formal request for a new account, specifying the user's role and required access level and Provides justification for account creation and ensures compliance with SnowBe policies.

Technical Consultant (external role):

The Technical Consultant provides expertise in identifying and mitigating risks, helping SnowBe Online implement the NIST 800-53 framework, as well as other industry best practices. This includes assisting with system hardening, process improvements, and deploying technical controls to address identified vulnerabilities.

Third Party Vendors:

Third-party vendors are responsible for adhering to SnowBe Online's security policies and contractual obligations. They must ensure the security of the services and systems they provide, cooperate during audits, and supply any required documentation to verify compliance with regulatory and contractual requirements.

Senior Director of IT Security and Assurance:

Responsible for the creating and overseeing this policy.

Senior Management:

Provide policy Approval and Oversight:

Approve the Least Privilege Policy and allocate resources for its implementation. Oversee compliance with the policy and ensure alignment with company objectives.

Section 5: Statement of Policies, Standards and Procedures

Policies

Access Control Policy:

The purpose of this document is to define policy and procedures SnowBe Online for implementing and maintaining appropriate access controls (see Definitions) for State information assets (see Definitions). This document corresponds to the Access Control Family of National Institute of Standards and Technology (NIST)Special Publication 800-53 (Rev. 4)

Backup/Disaster Recovery Policy:

Policy is to provide direction and general rules for the creation, implementation, and management of the SnowBe Online Technology Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

Bring Your Own Device Policy (BYOD):

The purpose of this Bring Your Device (BYOD) Policy is to establish guidelines and procedures for employees and contractors who wish to use their personal devices to access SnowBe Online corporate network and information assets. This policy contains rules, expectations, and an overall approach to ensure the security and integrity of corporate data while allowing the use of personal devices for work-related purposes.

Change Control Management Policy: This policy ensures that all changes to SnowBe's IT systems are managed efficiently to minimize disruptions, enhance security, and maintain compliance with NIST 800-53 r5 and PCI DSS.

Data Encryption Policy:

This policy outlines the guidelines for utilizing encryption to safeguard SnowBe's confidential information and personally identifiable information (PII), both when stored (at rest) and during transmission (in transit). It aims to ensure compliance with relevant regulations and to protect sensitive data from unauthorized access.

Data Protection Policy:

SnowBe Online is committed to protecting the privacy and security of personal data in accordance to applicable data protection laws and regulations. This Data Protection Policy outlines SnowBe Online's commitment to safeguarding personal data including how it is collected, processed, stored, and managed, which may include but not limited to:

- The Federal Data Protection Regulation (GDPR) in Europe
- The California Consumer Privacy Act (CCPA) in the United States
- The Personal Data Protection Act (PDPA) in Singapore
- The Privacy Act in Australia

This policy establishes the framework for responsibility collecting, processing, storing, and managing personal data in compliance with these laws.

Email Security Policy:
The purpose of the email security policy is to establish any standards for using company email systems to safeguard sensitive information. This is used to prevent unauthorized access as well as to ensure data confidentially as well as integrity.

Encryption Policy:
This policy outlines the guidelines for utilizing encryption to safeguard SnowBe's confidential information and personally identifiable information (PII), both when stored (at rest) and during transmission (in transit). It aims to ensure compliance with relevant regulations and to protect sensitive data from unauthorized access.

Equal Employment Policy:
An Equal Opportunities Policy is a set of guidelines designed to ensure that everyone is treated with fairness and respect in the workplace. This policy's intention is to prevent discrimination and ensure that all employees, regardless of race, age, gender, sexual orientation, disability, religion, or any other attribute, are treated equally when it comes to hiring, wages, promotions, and other job-related activities.

Malware Protection Policy:
The purpose of this policy is to protect organizational data and systems from any malicious software by implementing preventive measures, detecting potential threats and lastly responding effectively to incidents. Also, this is used as a safeguard for the organization's IT systems, data, as well as the users from malicious software like viruses. This policy also establishes guidelines that will prevent, detect, and respond to malware threats effectively.

Network Security Policy: The purpose of this policy is to delineate acceptable use of SnowBe Online's technology resources. These rules are in place to protect the user of these resources and SnowBe Online. Inappropriate use exposes SnowBe Online to risks including virus attacks, compromise of network systems and services, and legal issues.

Password Management Policy:
The purpose of this policy is to provide SnowBe Online and its users with guidelines for password creation and use. This policy will ensure that passwords are created with security in mind. This policy will provide guidelines on how to create a secure password and the importance of a secure password.

AC-2 Account Management:

This policy establishes guidelines and procedures for managing user accounts and privileges to ensure that access to SnowBe Online's systems, data, and resources is controlled, secure, and aligned with the principles of least privilege. It aims to protect sensitive information, prevent unauthorized access, and comply with industry standards such as PCI DSS and NIST 800-53.

AC-6 Least Privilege: The purpose of this policy is to enforce the principle of least privilege across SnowBe Online's information systems and resources. This principle ensures that users, applications, and devices are granted the minimum access necessary to perform their legitimate functions, minimizing potential security risks and ensuring compliance with relevant regulatory frameworks.

AC-17 Remote Access:

The purpose of this policy is to define standards for minimizing security risks that may result from unauthorized remote access to SnowBe's IT Resources

Standards and Procedures

Create New Account Procedure:

This procedure details the procedural steps, information, and considerations that are part of account creation and removal by SnowBe Online's IT team.

Password Standard:

Password requirements for standard accounts:

Passwords may never be stored in plain text. Passwords must be stored using industry standard hashing and salting methodologies.

Passwords must be encrypted and/or hashed while in transit to the authenticating system.

Passwords should not be displayed in plain text as they are being entered.

Passwords must adhere to the following complexity rules: ○ Passwords must be at least twelve (12) characters long.

The password must contain characters from three of the following four categories: ▪ Upper Case: A B C ...

▪ Lower Case: a b c ...

▪ Numbers: 1 2 3 ..

▪ Symbols: + - _ = . @ ? ! . . .

The password cannot contain any three consecutive characters that are part of your name or NetID.

Password requirements for administrative accounts:

In addition to the requirements for standard accounts:

-Passwords may not be re-used for a period of 12 months.

-Accounts must use Multi-Factor Authentication (MFA) where possible.

Password requirements for service accounts:

Service based accounts are those used for automation, monitoring, and other non-interactive tasks not performed by an individual.

In addition to the requirements for standard accounts.

- Passwords must be at least 16 characters.

- User IDs and passwords shall never be used through an interactive logon mechanism except for testing/setup purposes.
- Service accounts must have a responsible point of contact or sponsor.
- Service accounts must be reviewed annually to ensure they are properly used, secured, and necessary.

Initial Account Provisioning:

Newly provisioned user accounts must have a secure password set by the account holder. This may be accomplished via an activation method that allows the account holder to set a password (before which the account is not usable), secure transmission of an initial password to the account holder, a small expiration window for an initial password, and/or manual intervention of support resources.

If an initial account password is set before account handoff to the account holder:

Account holders must have the ability to either activate an account and set a password before use or require users to set a password during initial access to a system. Service accounts may be considered exempt from this requirement.

All vendor-supplied passwords, including service accounts, must be changed as soon as possible after system/application deployment and before becoming operational.

Password Protection:

To ensure that the intended account holder is the authorized holder of a password or credential, distribution or reset should occur only after reasonable effort has been made to verify the identity of the account holder.

Individuals should be confirmed as the intended recipient by contact via an authorized work phone number, verification of personal data, photo ID, or similar means.

Where possible, passwords should be maintained by the individual through automated means that leverages either preexisting answers to a set of questions or through the use of a secondary channel meant to confirm someone's identity, such as a one-time password sent to a registered person's device. If an automated process is not available, initial or reset passwords may be communicated via:

Mail (sealed envelope)
Encrypted file transfer (e.g., Filelocker or similar)
Verbal conversation, either a phone call to authorized work telephone number or in-person communication

Password Procedure:

All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.

- All production system-level passwords must be part of the Information Security administrated global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- User accounts with access to SnowBe Online privileges must have a unique password from all other accounts held by that user. • Passwords must not be inserted into email messages or other forms of electronic communication.

- Where simple network management protocol (SMTP) is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system" and must be different from passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

Passwords are used for various purposes at SnowBe Online. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., Dynamic passwords which are used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:

< Name of family, pets, friends, co-workers, fantasy characters, etc.
< Computer terms and names, commands, sites companies, hardware, software.
< The words "SnowBe Online"," "WVSP," "HPD," "CKSFP" or any derivation.

< Birthdays and other personal information such as addresses and phone numbers. < Word or number patterns like aaabbb, 111222, zyxwvts, 4654321, etc.

< Any of the above spelled backward like nhoj, yrrehckcalb, yffulf, etc. < Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z) • Have digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+{}[]:";<>?,.?
- Are at least eight alphanumeric characters long.
- Are not a word within any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords

4.3 Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

< When a user retires, quits, is reassigned, released, dismissed, etc.

< Default passwords shall be changed immediately on all equipment.

< Contractor accounts, when no longer needed to perform their duties. When a password is no longer needed, the following procedures should be followed:

< Employee should notify his or her immediate supervisor.

< Contractor should inform his or her point-of-contact (POC).

< Supervisor or POC should fill out a password deletion form and send it to <SnowBe Online's IT Director>.

< SnowBe Online's IT Director will then delete the user's password and delete or suspend the user's account.

< A second individual from that department will check to ensure that the password has been deleted and user account was deleted or suspended. < The password deletion form will be filed in a secure filing system.

4.4 Password Protection Standards

Do not use your user id as your password. Do not use the same password for SnowBe Online accounts as for NCIC accounts. For example, select one password for your Windows account login and a different one for your NCIC account login. Do not share SnowBe Online's passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential SnowBe Online information.

Here is a list of "do nots"

< Don't reveal a password over the phone to anyone

< Don't reveal a password in an mail message

< Don’t reveal a password to the boss
< Don’ talk about a password in front of others
< Don’t hint at the format of a password (e.g., “my family name”)
< Don’t reveal a password on questionnaires or security forms
< Don’t share a password with family members
< Don’t reveal a password to a co-worker while on vacation
< Don’t use the "Remember Password" feature of applications
< Don’t write passwords down and store them anywhere in your office. < Don’t store passwords in a file on ANY computer system without encryption.

If someone demands a password, refer them to this document or have them call <list name of Information Security Officer (ISO) or Agency POC.

If an account or password is suspected to have been compromised, report the incident to the IT Director and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the FBI If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide some sort of role management, such that one user can take over the function of another without having to know the other’s password.
- Should support Terminal Access Controller Access Control System+ (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

D. Remote Access Users

Access to the SnowBe Online’s networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

Section 6: Exceptions/Exemptions

•Requests must be formally submitted to the IT Director, specifying the security controls affected.

•Following submission, the request will be reviewed by senior management and the legal team. If approved, the exception will be temporary, lasting up to 45 days.

•During this exception period, the IT team will implement necessary risk mitigation measures and monitor for any escalating risks.

•After 45 days, the exception will either expire, necessitating a return to full compliance, or the request will be reassessed for a potential extension.

•If no extension is granted, the IT team will ensure all temporary adjustments are removed and that the system fully adheres to the original security controls

Emergency circumstances:
In very urgent situations such as a system recovery, there should be certain security protocols that might need to be temporarily bypassed. If this situation occurs, it must be clearly documented and justified as to why it was performed.

Role-based exceptions:
In specific rules such as the system administrators, they might need exceptions to standard rules. An example of this could be broader access to the systems. These roles could come with additional oversight and security measures and must be used with proper documentation.

Third-Party services:
If a third-party would happen to be needed a security plan must allow for that specific service. This is only if the provided met predefined security standards as well as passed audits.

Section 7: Version History Table

Version	**Date**	**Description**
V1	12/02/24	Development of Initial sec. plan

V2	12/05/24	Addition of policies and definitions
V3	12/11/24	Addition of policies and corrections to format
V4	12/21/24	Finalization of document

Citations

https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

https://linfordco.com/blog/information-security-roles-responsibilities/

https://www.cisa.gov/sites/default/files/publications/ISC-Facility-Security-Plan-Guide-2015-508.pdf

https://Termsfeed.com/blog/gdpr-data-protection-policy/

https://www.sciencedirect.com/topics/computer-science/encryption-policy

https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf

https://technology.howard.edu/sites/technology.howard.edu/files/2020-03/NetworkSecurityPolicy_UPC_0.pdf
https://policy.tennessee.edu/procedure/gp-001-02-security-exceptions-and-exemptions-to-its-standardspractices-controls/

https://policy.tennessee.edu/procedure/gp-001-02-security-exceptions-and-exemptions-to-its-standardspractices-controls/

https://www.neweratech.com/us/wp-content/uploads/sites/5/2024/11/Business-Continuity-andDisasterRecovery-Policy.pdf https://www.sciencedirect.com/topics/computerscience/encryptionpolicy

https://www.fortinet.com/resources/cyberglossary/byod

Team, Easy Legal Docs Editorial. "Equal Opportunities Policy Template - Free Download." Easy Legal Docs, 3 Apr. 2024, easylegaldocs.com/templates/policies/equal-opportunities-policy/.

"EEO Policy Statement." US EEOC, www.eeoc.gov/eeo-policy-statement. Accessed 3 Dec. 2024. Dun &

Bradstreet - Accelerate Growth and Improve Business Performance, www.dnb.com/content/dam/english/company/Privacy_and_Personal_Data_Protection_Policy.pdf. Accessed 3 Dec. 2024.

https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/it-resources-remote-access-policy/ https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-andguidelines/wireless-use-policy/

https://www.bmc.com/blogs/change-management-roles/ https://www.carrtegra.com/2015/12/roles-responsibilities-change-management-process/

https://www.gntc.edu/fullpanel/uploads/files/accountcreationprocedures.pdf

https://aws.amazon.com/compliance/shared-responsibility-model/

https://learn.microsoft.com/en-us/partner-center/account-settings/create-user-accounts-and-set-permissions

https://www.dictionary.com/
https://rockvalleycollege.edu/_resources/files/procedures/2-30-060-Procedure-Passwords.pdf
https://dojmt.gov/wp-content/uploads/Password-Policy-and-Procedure-Example.pdf
https://www.techtarget.com/searchsecurity/tip/How-to-create-a-company-password-policy-with-template
https://policy.illinoisstate.edu/technology/9-2-2/

https://security.uconn.edu/password-standards/ https://www.mtu.edu/it/security/policies-proceduresguidelines/information-security-program/password-standards/
https://www.ibm.com/docs/en/sim/7.0.2?topic=administration-password-policies