SnowBe Security Plan

SNOWBE ONLINE

Thomas Ayres

9/5/22 | V1.3

Table of Contents

Introduction 2

Scope 2

Definitions........ 2

Roles & Responsibilities 3

Statement of Policies 3

Password Policy 3

Information at Rest........ 5

Transmission Confidentiality and Integrity........ 6

Change Management/Control 7

PCI DSS 10

Physical Security 11

System Maintenance........ 12

Account Management........ 13

Remote Access........ 14

Standards and Procedures 16

Creating a New Account 16

Selecting a new Password 16

Resources 18

Version History........ 18

Introduction

This document is in place to guide SnowBe online to a place of better security and peace of mind. Given our increased popularity, it is crucial to provide a safe shopping experience for our customers. Within this document you will find polices in place to meet the compliance needs required for standards like PCI DSS and others.

Scope

This security plan applies to the faculty, networks, systems, facilities, devices, and any third-parties that are applicable to SnowBe Online.

Definitions

Attack Surface *- The devices, services, and configurations that threat actors may examine for vulnerability or implementation weaknesses.*

Server Firmware *- The operating system installed on server hardware that hosts services on the network.*

CISO *- Chief Information Security Officer. The person in charge of overseeing the aspects of security within company information technology.*

Insider Threat *- The possibility that an employee may turn malicious and act against the company to procure data or to disable critical hardware.*

Cardholder *- An individual who uses a payment card.*

Cardholder Data *- Data pertaining to a payment card. This includes the card holder name, the number, and the security code.*

PCI DSS *- Payment Card Industry Data Security Standard. The founding standard behind payment card data security.*

Remote Access *- Access to company infrastructure and networks from an authorized device from an outside network.*

Information at Rest - *Data that is not actively being transmitted that typically contains information like account data, customer health information, customer profile information, etc.*

Confidentiality *- Ensuring that only the intended parties can view, alter, and store specific data.*

Integrity *- Verifying that data and information has not been tampered with or corrupted.*

Roles & Responsibilities

***Account Management Officer** - In charge of monitoring any automated or manual systems, creating and deleting user accounts, making changes, and maintenance.*

***Information Technology Technician** - In charge of working with laptops and the company's internal network for proficient and secure methods of remote access between the two. In charge of working with all database servers, workstations, and mobile devices to ensure proper up-to-date encryption is in place for the integrity and confidentiality of all stored SnowBe company data.*

***HR Associate** - Set the proper roles, responsibilities, and access permissions for all new employees during the hiring process.*

Statement of Policies

Password Policy

Purpose:

Assigning unique user logins and requiring password protection is one of several primary safeguards employed to restrict access to the Weill Cornell Medicine network and the data stored within it to only authorized users. If a password is compromised, access to information systems can be obtained by an unauthorized individual, either inadvertently or maliciously. Individuals with CWIDs are responsible for safeguarding against unauthorized access to their account, and as such, must conform to this policy in order to ensure passwords are kept confidential and are designed to be complex and difficult to breach. The parameters in this policy are designed to comply with legal and regulatory standards, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS). [reference 4]

Scope:

This policy pertains to all SnowBe employee user account passwords and password handling.

Policy:

*1. **Individual Responsibilities***

Individuals are responsible for keeping passwords secure and confidential. As such, the following principles must be adhered to for creating and safeguarding passwords:

- *WCM passwords must be changed immediately upon issuance for the first-use. Initial passwords must be securely transmitted to the individual.*

- *WCM passwords must never be shared with another individual for any reason or in any manner not consistent with this policy. A shared or compromised CWID password is a reportable ITS security incident.*

- *Employees—including faculty, physicians, and supervisors—as well as students and other WCM personnel, must never ask anyone else for their password. If you are asked to provide your password to an individual or sign into a* *system and provide access to someone else under your login, you are obligated to report this to the Privacy Office or ITS Security using one of the methods outlined in the Procedures section below.*

• *WCM passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats on untagged (unsupported) devices. Passwords may be stored in a secure password manager, such as LastPass, as long as the master password is kept private and meets the requirements in the 3.Password Requirements section of this policy.*

• *Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.*

 To access shared workstations (e.g., clinical exam rooms, kiosks), ITS will provide a limited-use shared account for the workstation. Individual credentials must then be used for accessing applications, such as Epic.

 ITS will never ask for a password. In ITS support scenarios where an ITS account cannot be used, an individual may allow a technician to utilize his/her computer under the individual's account even if the individual is unable to be present during the entire support session. The individual should not share his/her password with the technician. All ITS support technicians are expected to abide by the ITS 11.01 – Responsible Use of Information Technology Resources policy and their actions may be audited upon request.

 In the event of a hardware malfunction and the device needs to be repaired by a third-party, the device hard drive should be backed up to a secure storage device and wiped securely prior to being handed over to an external technician. ITS can assist with a secure backup and the drive erasure and other exceptional circumstances. Passwords should not be shared with an external technician.

• *In the event that a password needs to be issued to a remote user or service provider, the password must be sent with proper safeguards (e.g., shared via a secure password manager or sent via an encrypted email message).*

• *If a password needs to be shared for servicing, ITS Security should be contacted for authorization and appropriate instruction.*

• *Passwords for WCM must be unique and different from passwords used for other personal services (e.g., banking).*

• *WCM passwords must meet the requirements outlined in this policy.*

• *WCM passwords must be changed at the regularly scheduled time interval (as defined in 4.Password Expiration where applicable) or upon suspicion or confirmation of a compromise.*

• *Individuals with access to service accounts or test accounts must ensure the account password complies with this policy and must keep the password stored in a secure password manager.*

• *In the event a breach or compromise is suspected, the incident must be reported to ITS Security immediately using one of the methods outlined in the Procedures section below.*

reference [4]

*2. **Responsibilities of Systems Processing Passwords***

All WCM systems—including servers, applications, and websites that are hosted by or for WCM—must be designed to accept passwords and transmit them with proper safeguards.

- *Passwords must be prohibited from being displayed when entered.*

- *Passwords must never be stored in clear, readable format (encryption must always be used).*

- *Passwords must never be stored as part of a login script, program, or automated process.*

- *Systems storing or providing access to confidential data or remote access to the internal network must be secured with multifactor authentication.*

- *Password hashes (irreversible encoded values) must never be accessible to unauthorized individuals.*

- *Where possible, salted hashes (irreversible encoded values with added randomness) should be used for password encryption.*

- *Where any of the above items are not supported, a variance request should be submitted to ITS for review. Appropriate authorizations and access control methods must be implemented to ensure only a limited number of authorized individuals have access to readable passwords.*

*3. **Password Requirements***

The following parameters indicate the minimum requirements for passwords for all individual accounts (except for passcodes defined in section 6. Mobile Devices) where passwords are:

- *At least sixteen (16) characters;*

- *Not based on anything somebody else could easily guess or obtain using person-related information (e.g., names, CWID, telephone numbers, dates of birth, etc.); and,*

- *Not vulnerable to a dictionary attack (see section 7. Recommendations for Creating Compliant Passwords).*

Information at Rest

Purpose

Protect the [Selection (one or more): confidentiality; integrity] of the following

information at rest: [Assignment: organization-defined information at rest].

[NIST 800-53r5, pg.316]

Scope

This policy concerns all data that is stored on SnowBe workstations, physical databases, cloud databases, and issued mobile devices.

Policy

Information at rest refers to the state of information when it is not in process or in

transit and is located on system components. Such components include internal or external hard *disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage. [NIST 800-53r5, pg. 316]*

Enhancements

(1) Cryptographic Protection - This enhancement is like the enhancement for SC-8, except that it deals with data that is being stored. This enhancement is to make sure that the integrity and confidentiality of resting data is protected by using up to date encryption on the data, to make sure that third parties cannot do anything with compromised data. [NIST 800-53r5, pg. 317]

Enforcement

This is to be tackled before the beginning of Q3, so that PCI compliance can be achieved.

Transmission Confidentiality and Integrity

Purpose

Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.

Scope

All internal company infrastructure to-and-from workstations, databases, payment card systems, company mobile devices, and IoT devices.

Policy

Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, *including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fiber-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques. Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls. [NIST 800-53r5, pg. 304]*

Enhancements

(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION - Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPsec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes. [NIST 800-53r5, pg. 305]

Enforcement

Due to its importance, enforcement of this policy will be in place before the beginning of Q3.

Change Management/Control

Purpose

The purpose of this policy is to manage changes in a well-communicated, planned, and predictable manner that minimizes unplanned outages and unforeseen system issues. Effective change management requires planning, communication, monitoring, rollback, and follow-up procedures to reduce negative impact to the user community.

Scope

This policy applies to all staff involved in application or systems changes, updates, or patches.

Roles and Responsibilities

Management - In charge of enforcing the contents of this policy, chain of command style, so that change in SnowBe's policies, infrastructure, employees, and process may be transitioned to as smoothly as possible.

Policy

All system and application changes in [Insert Appropriate Department] (e.g. operating system, computing hardware, networks, applications, data centers) are subject to this policy and shall follow unit change management procedures.

The following general requirements shall be met in the change management process:

- *Scheduled change calendars and departmental communications operational procedures shall be developed to inform stakeholders of upcoming application and system changes that impact system availability or operations*

- *Regular planned changes shall minimally be communicated to all stakeholders monthly through a communication mechanism of the [Insert Appropriate Role]'s choosing*

- *Unplanned outages shall be communicated immediately to stakeholders with regular updates on progress towards resolution and resumption of service*

- *Regular system and application patching schedules shall be communicated to users and performed in such a way as to minimize system downtime and user productivity*

- *Changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) shall be reported to or coordinated with [Facilities] and stakeholders shall be notified through [Insert Appropriate Department] change management communications*

- *Processes shall ensure that production data is not unnecessarily replicated or used in non-production environments*

- *Device configurations shall be backed up and rollback procedures must exist prior to implementing a change*

[ref. 1]

CHANGE MANAGEMENT COMMITTEE

A [LEP] Change Management Committee shall convene to discuss system changes, interactions, and any perceived issues. This committee shall be made up of network and systems staff, application development owners, developers, and chaired by the [Insert Appropriate Role] or their designee. The following procedures shall be implemented by the committee:

The committee shall meet on a schedule determined by the [Insert Appropriate Role] but shall minimally meet monthly to discuss plans for future updates and patching. [ref.1]

CHANGE REQUEST MANAGEMENT

The following procedure shall be implemented surrounding the change management process:

- *Change requests shall be submitted for all changes, both scheduled and unscheduled*

- *All scheduled change requests shall be submitted in accordance with departmental change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the system update*

- *Change requests shall receive Change Management Committee approval before proceeding with the change*

- *A change review must be completed for each change, whether scheduled or unscheduled, and whether successful or unsuccessful*

[ref.1]

CHANGE MANAGEMENT DENIALS

The [Insert Appropriate Role] or their designee may deny a scheduled or unscheduled change for reasons including, but not limited to:

- *Inadequate change planning or unit testing*

- *Lack of stakeholder acceptance (where applicable)*

- *System integration or interoperability concerns*

- *Missing or deficient roll-back plans*

- *Security implications and risks*

- *Timing of the change negatively impacting key business processes*

- *Timeframes do not align with resource scheduling (e.g. late-night, weekends, holidays, or during special events)*

[ref.1]

ADMINISTRATION

A Change Management Log Form shall be maintained for all changes. This log must contain, but is not limited to:

- *Date of submission and date of change*

- *Owner and custodian contact information*

- *Nature of the change*

- *Indications of success or failure*

- *Notes and follow-ons*

[ref.1]

Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP]. Satisfactory examples of evidence and compliance include:

- *Historical logs of change events*
- *Archival Change Management Committee meeting minutes*
- *Anecdotal documentation and communications showing regular compliance with the policy*

[ref.1]

Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination. Policy is effective immediately.

PCI DSS

Purpose

This policy is to align SnowBe with the standards held by the PCI DSS for payment card data. Failure to comply with these standards can result in fines, damage to company reputation, inability to use card payment, financial strain on the customer, and the further disappointment of your father.

Scope

This policy will apply to those who handle cardholder data. This includes employees, vendors, systems, and those associated with SnowBe.

Roles & Responsibilities

***Faculty** - Protect cardholder data, report all instances of fraud or scam to a manager.*

***IT Department** - Keep technology and configurations up to date with most recent PCI standards. Verify properly encrypted transmission of data and encrypted storage of data.*

Policy

Goals	***PCI DSS Requirements***
Build and Maintain a Secure Network and Systems	*1. Install and maintain a firewall configuration to protect cardholder data* *2. Do not use vendor-supplied defaults for system passwords and other security parameters*
Protect Cardholder Data	*3. Protect stored cardholder data*

	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	*5. Protect all systems against malware and regularly update anti- virus software or programs* *6. Develop and maintain secure systems and applications*
Implement Strong Access Control Measures	*7. Restrict access to cardholder data by business need to know* *8. Identify and authenticate access to system components* *9. Restrict physical access to cardholder data*
Regularly Monitor and Test Networks	*10. Track and monitor all access to network resources and cardholder data* *11. Regularly test security systems and processes*
Maintain an Information Security Policy	*12. Maintain a policy that addresses information security for all personnel*

Physical Security

Purpose

Physical security is a necessity any time that company-critical infrastructure is hosted directly. Having measures in place around servers and workstations goes a long way to reduce insider threat as well as malicious activity from the public.

Scope

Any server infrastructure, or employee workstations, that are hosted within or around SnowBe facilities.

Roles & Responsibilities

A higher member of the IT or Cybersecurity team can perform this assessment. Given the nature of this policy, it is the responsibility of the assessor to relay the needed changes or improvements to the CISO, who will be in contact with the financial department.

Policy

Questions	*Severity 1-10, 10 being most severe*	*Initial box if applicable*
Is the server room inaccessible to the public and to general employees?	*10*	
Is the server room secured with materials not easily broken?	*7*	

Is the server room secured with multi-factor authentication and reputable locks?	*7*	
Are employee desktop cases secured from internal access?	*5*	

Exceptions/Exemptions

Given the questionnaire, remediation should be apparent based upon the importance of the items.

Enforcement

Physical security is to be assessed and acted upon annually, in the beginning of the business year.

System Maintenance

Purpose

System Maintenance is important to protect a system or network against risk factors. Consider consistent updates and assessment of network devices to be a crucial part in reducing the overall attack surface of business infrastructure.

Scope

There are twenty desktops, thirty laptops, and six servers within the scope of this network. Within these devices, the following items are to be addressed: server firmware, backup software, anti-virus software, and the WordPress web application shopping cart. These items are to be updated to the most recent and stable LTS versions.

Roles & Responsibilities

Through the CISO, officers in charge of this project will be delegated and in charge of updating specific classifications or sections of devices within the company. These officers' responsibilities will involve the successful implementation of all software updates before the end of month one within their specified scope.

Policy

Antivirus Software *- fully updated to the most recent version.*

Workstation Firmware *- Updated to the most recent known compatible version.*

Server Firmware *- Updated to the most recent known compatible version.*

Server Backup Software *- Updated to the most recent version.*

Web Application Functionality *- Address vulnerable or outdated code.*

Exceptions/Exemptions

Hardware and software that are running infrastructure-critical services are not to be touched until the load can be shifted temporarily as to keep public services available.

Enforcement

This policy is to be enforced biannually, once within the beginning of Q2 and again in the beginning of Q4.

Account Management

Purpose

The purpose of Account Management is to manage a userbase and assign roles, responsibilities, and access controls. It also deals with logging, proper creation/deletion of accounts, and the locking down or pausing of accounts.

Scope

All user accounts whether customer, employee, chief management, or otherwise need to follow the storage, access, creation, and removal guidelines laid out in this policy.

Definitions

Account Management *- Moderating the creation, deletion, roles, capabilities, and information surrounding user accounts.*

Policy:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;

d. Specify:

1. Authorized users of the system;

2. Group and role membership; and

3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;

e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];

g. Monitor the use of accounts;

h. Notify account managers and [Assignment: organization-defined personnel or roles] within:

1. [Assignment: organization-defined time period] when accounts are no longer required;

2. [Assignment: organization-defined time period] when users are terminated or transferred; and

3. [Assignment: organization-defined time period] when system usage or need-to-know *changes for an individual;*

i. Authorize access to the system based on:

1. A valid access authorization;

2. Intended system usage; and

3. [Assignment: organization-defined attributes (as required)];

j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

Reference: [NIST, pg. 46]

Control Enhancements:

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

Reference: [NIST, pg. 47]

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

Reference: [NIST, pg. 48]

Enforcement

The company-assigned Account Management Officers are to have the system in place by the end of Q2 / Beginning of Q3.

Remote Access

Purpose

Devices that leave a well-protected network can be prone to many threats from the world outside that leave the internal network vulnerable. There are many ways to prevent this, however, and it is the goal of this policy to ensure that all SnowBe company devices that are used within the scope of remote-access work can connect to our internal network securely, while also keeping our network uncompromised from potential threat.

Scope

All SnowBe company laptops that are designated for remote online work and are having to leave the premises on a regular basis must adhere to the policy specified by this document.

Policy:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections. Discussion: Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-3. Enforcing access restrictions for remote access is addressed via AC-3.

Reference: [NIST, pg. 48]

Control Enhancements:

(1) REMOTE ACCESS | MONITORING AND CONTROL

Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.

Reference: [NIST, pg. 48]

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

Reference: [NIST, pg. 49]

Enforcement

Information Technology Technicians will need to accomplish the guidelines within the policy by the end of Q4.

Standards and Procedures

Creating a New Account

Purpose

To grant the proper roles, responsibilities, and access to those who are freshly entering the company.

Scope

All new employees need to be registered under this process before starting work at SnowBe Online.

Procedure

Automated:

> Place employee information into automated account-creatin' software

Manual:

> Fill out everything manually

> Verify roles with respective department head

> Double check that access controls are correct

> Cry at your desk, because your management doesn't love you enough to buy the automated software

Enforcement

Starting now, policy is a go! Enforced as of right now or we will fire the entire HR department.

Selecting a new Password

Guidelines for Selecting Good Passwords:

The responsibility for effective password management is shared by all users of the university s computing and communications resources and begins with selecting good passwords. To assist in this process, consider the following general guidelines:

- *Good passwords are passwords that are difficult to guess. So, consider mixed passwords that contain a combination of letters and numbers. Use a leading character(s) separated by a number or special character.*

- *Use a phrase or sentence to assist you in remembering character strings. Add a number or symbol. Mixing case is an excellent way to create a strong password. (NOTE: Some systems may not allow for mixed case.)*

- *NEVER share your personal passwords! Do not give out your passwords to IT or system personnel during help sessions. The password is your protection that only you have authentic access to your data and data owned by the university.*

[reference 3]

Good passwords:

- *Have both upper- and lower-case letters*
- *Have digits and/or special characters as well as letters*
- *Are easy to remember, so they do not have to be written down*
- *Are at least 6 characters long*

Passwords on multiple machines: If you have several computer accounts, you may wish to have the same password on every machine. However, if you have the same password on many machines and one of those machines is compromised, all of your accounts are compromised. One common approach is to have a base passoword and add to it a number or letter that represents the machine you are using. Use a method that is best for you.

Since length and composition of passwords, time between password changes and number of login attempts sometimes vary between systems, call the numbers listed above if you need additional information on password standards.

[reference 3]

Password Requirements:

Individuals using University computer systems must assure effective password/information security management by being aware of and following the password management standards for each system they access. Most notably, this means choosing strong passwords and safeguarding their integrity.

Computer passwords represent an individual's identity to the system and must never be disclosed or used by others. Unauthorized use of a computer ID is a violation of University policies relating to password management, Information Security and Appropriate Use of Information Technology Resources. Violations of these policies are punishable under University Employee Standards of Conduct, faculty, employee and student handbooks, and the University honor and judicial systems. Violations of standards for password management and information security may result in dismissal from the University or other remedies. State and federal laws may also apply.

- *Requesting, Modifying, Retiring Accounts/Passwords*

Employees, in consultation with their supervisors, can request computer IDs and privileges consistent with their responsibilities at the University (see Procedure on Requesting a User ID). As these responsibilities change, supervisors must request the appropriate access changes.

Moreover, as individuals leave, change positions, or change responsibilities within the University, supervisors must immediately notify IT, so that accounts can be disabled. Full-time employees are to complete the Employee Clearance process as they terminate employment.

In addition to the password management standards outlined below, computer accounts for all temporary employees are subject to expiration every 60 days. If a request for account renewal is not submitted by the temporary employee's supervisor, prior to the end of the 60 day period, the account will be disabled.

[reference 3]

Resources

1.) [Link to change management policy]

2.) [NIST 800-53r5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

3.) https://www.jmu.edu/itplan/policy/pwmgtpro.html

4.) https://its.weill.cornell.edu/policies/1115-password-policy-and-guidelines

Version History

Version Number	Description	Date
0.1	Initial Template	9/4/22
1.0	Initial Security Plan	9/6/22
1.1	Added new policies	9/12/22
1.2	Added three new policies and a procedure.	9/19/22
1.3	Added password policy and procedure.	9/25/22