SNOWBE ONLINE SECURITY PLAN

Adam Duckworth, Yaseen Al-Azzawi, and Jordan Bohling - VERSION # 4.0 October 22, 2023

Table of Contents

Section 1: Introduction

Information security is essential to the mission of SnowBe Online and is a company-wide responsibility. The SnowBe Online Information Technology Security Plan defines the information security standards and procedures for ensuring the confidentiality, integrity, and availability of all information systems resources and data under the control of SnowBe. The purpose of this security plan is to provide an overview of the security requirements of the IT system and describe the controls in place or planned for meeting those requirements.
Furthermore, the company recognizes its responsibility to promote security awareness among the employers and third-party vendors of SnowBe Online. The objective of the security plan is to improve the protection of IT resources.

Section 2: Scope

SnowBe Online is responsible for protecting the confidentiality, integrity, and availability of company information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the integrity of the mission of SnowBe, violate individual privacy rights, and possibly constitute a criminal act. It is the collective responsibility of all users to ensure they are familiar with and adhere to SnowBe policies, including privacy, acceptable use of information technology resources, and other facilities and property policies.
This plan applies to any use of the company's computing or network resources as defined in facilities and property policies. Additional standards and procedures may govern specific data or computer systems or networks provided or operated by third-party service providers and vendors. This plan applies to all company personnel and entities and is to be read by all company technical support staff and information asset owners.

Section 3: Definitions

Application encryption - Encryption of files or fields of data at the application level.

Availability - the level of assurance that authorized users have access to information resources when required.

Blogging - Add new material to or regularly update a blog.

Cardholder - Individual who owns and benefits from the use of a membership card, particularly a payment card.

Cardholder Data (CHD) - Elements of payment card information that must be protected, including primary account number (PAN), cardholder name, expiration date, and the service code.

Cardholder Name - The name of the individual to whom the card is issued.

CAV2, CVC2, CID, or CVV2 data - The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

Certificate revocation - A process in which a certificate is deemed invalid before the end of its lifecycle.

Ciphertext - Encrypted data transformed from plaintext using an encryption algorithm.

Cipher suites - A set of algorithms that help secure a network connection.

Confidentiality - refers to the level of assurance that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Contractor - Someone officially attached or connected to SnowBe Online who is not an employee.

Control - Process or procedure to reduce risk.

Criticality - the relative importance of the information to the mission of SnowBe and reflects the degree to which the information requires protection to ensure it is not accidentally or maliciously altered or destroyed.

Cryptography - The science of protecting information by transforming it into a secure format.

Cryptographic keys - A string of data that is used to lock or unlock encrypted data.

Database encryption - Encryption of data types, fields, or entire datasets at the database level.

Data at rest - Data that is stored on a hard drive or other media and not actively moving from device to device or over a network.

Data in transit - Data that is in motion and being transmitted across a network between devices.

Deprovisioning - The act of removing user access to applications, systems, and data within a network. It's the diametric opposite of provisioning, which grants, deploys, and activates services for users in a system.

Disposal - CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, and USB storage devices. The approved PCI DSS disposal methods include cross-cut shredding, incineration, and approved shredding and disposal service.

Encryption - The process of converting data to an unrecognizable format, called ciphertext so that only authorized parties can view it.

Encryption algorithms - The method used to transform data into ciphertext. An algorithm will use the encryption key to alter the data in a predictable way so that even though the encrypted data will appear random, it can be turned back into plaintext by using the decryption key.

Expiration Date - The date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card.

File encryption - A method that encrypts individual files.

Full disk encryption - A cryptographic method that applies encryption to the entire hard drive including data, files, the operating system, and software programs.

Honeynet - A decoy network that contains one or more honeypots.

Honeypot - Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you are running vulnerable services that can be used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

Information Asset - data, system, computer, network device, document, or any other component of the university infrastructure which stores, processes or transmits data.

Information Security Risk Management (ISRM) - a program that consistently identifies, and tracks information security risks, implements plans for remediation, and guides strategic resource planning.

Information System: An individual or collection of computing and networking equipment and software used to perform a discrete business function. associated PC or the set of desktop computers used to perform general duties in a department.

Inherent Risk - The level of risk before Risk Treatments (controls) are applied.

Integrity - the assurance that information is not accidentally or maliciously altered or destroyed.

IT Resources - Include computing, networking, communications, application, and 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.

Magnetic Stripe (i.e., track) data - Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.

Merchant - A department or unit (including a group of departments or a subset of a department) approved to accept payment cards and assigned a merchant identification number.

Patch - a software update comprised of code inserted (i.e., patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited to the following:

Updating software
Fixing a software bug
Installing new drivers
Addressing new security vulnerabilities
Addressing software stability issues

Patch management cycle - a part of lifecycle management and is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.

Payment Card Industry Data Security Standards (PCI DSS) - The security requirements defined by the Payment Card Industry Data Security Standards Council and the major credit card brands including Visa, MasterCard, Discover, American Express, and JCB.

PCI Compliance Committee - Group composed of representatives from Financial Management, Information Security Office, Office of the Vice President and Chief Information Officer, Internal Audit, and UB merchants.

Personally Identifiable Information (PII) - any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

Physical Security - Security measures designed to deny unauthorized access to facilities containing IT Electronic Resources and protect personnel and property from damage or harm.

PIN or PIN block - Personal identification number entered by the cardholder during a card- present transaction, or encrypted PIN block present within the transaction message.

Plaintext - Unencrypted data.

Primary Account Number (PAN) - Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.

Privileged Access - Access that allows an individual who can take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, or other such employees whose job duties require access to sensitive data residing on a system or network. This data can be paper or electronic data. For the purposes of this policy, applications and other developers are also considered privileged.

Proprietary Information - Proprietary information is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.

Provisioning - the process of creating and setting up IT infrastructure, and includes the steps required to manage user and system access to various resources. Provisioning is an early stage in the deployment of servers, applications, network components, storage, edge devices, and more.

Ransomware - A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.

Residual Risk is a level of risk that remains after Risk Treatments (controls) are applied to a given Risk.

Restricted/Controlled Area – Any area not open to the public containing IT Electronic Resource

Risk is the possibility of suffering harm or loss or the potential for realizing unwanted negative consequences of an event.

Risk Assessment is the process of taking identified risks and analyzing their potential severity of impact and likelihood of occurrence.

Risk Management is the ongoing management process of assessing risks and implementing plans to address them.

Risk Treatment is the process of managing assessed or identified risks. Risk treatment options are risk avoidance (withdraw from), sharing (transfer), modification (reduce or mitigate) and retention (acceptance).

Security Awareness Training - a formal process for educating employees about the internet and computer security. A good security awareness program should educate employees about company policies and procedures for working with information technology (IT).

Security Safeguards - protective measures prescribed to meet security requirements (i.e., confidentiality, integrity, availability) specified for an information asset or environment. Also called security controls or countermeasures.

Self-Assessment Questionnaire (SAQ) - Validation tools to assist merchants and service providers report the results of their PCI DSS self-assessment.

Sensitive Authentication Data - Additional elements of payment card information required to be protected but never stored. These include magnetic stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data, and PIN or PIN block.

Sensitive Information - information whose unauthorized disclosure may have a serious adverse effect on the company's reputation, resources, services, or individuals. Information protected under federal or state regulations or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive.

Sensitivity - the degree to which information requires protection to ensure it is not exposed to unauthorized users.

Service Code - Permits where the card is used and for what.

SnowBe Online Data: Data in any format collected, developed, maintained or managed by or on behalf of SnowBe Online, or within the scope of company activities. The terms 'data' and 'information' are used interchangeably in the context of the information security program

Spam: Electronic junk mail or junk newsgroup postings.

Unit - any organization across SnowBe.

User Access Rights - Permissions each individual user has to company applications and resources such as printers, computers, and online file storage.

Section 4: Roles & Responsibilities

All users, including SnowBe employees and third-party contractors - Responsible for protecting SnowBe's information, adhering to all relevant policies, guidelines, and procedures, and making informed decisions to protect the information that they process.

Business or System Owners - Alignment to this policy and any related standards.

Chief Technology Officer (CTO): is responsible for SnowBe's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.

Control Owners - Responsible for defining and implementing change management procedures that meet or exceed the minimum requirements that have been established by this policy.

Data Custodians: have a responsibility to SnowBe Online to ensure they grant access to data to only those who require that access to perform their job responsibilities.

Data Owners: are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of information technology resources and data they own.

Data User: a person who has been granted explicit authorization to access the data by the owner. The user must use the data only for purposes specified by the owner, comply with security measures specified by the owner or custodian (i.e., securing login-ID and password), and not disclose information or control over the data unless specifically authorized in writing by the owner of the data.

Employees of SnowBe – Responsible for safeguarding cardholder data, reporting occurrences of possible incidents and data breach management, and reviewing and complying with Security and Awareness Training

Financial Management – Responsible for keeping current with PCI DSS regulations and making changes to processes (as appropriate), maintaining the inventory of all SnowBe devices, merchant ids, and terminal ids along with activation status, and evaluating compliance with PCI as part of scheduled cash handling reviews; this is a shared responsibility with Policy, Compliance and Internal Control.

Information Security Board of Reviews (ISBR): is to provide oversight and direction regarding information systems security and privacy assurance company-wide.

Information Security Manager - has delegated responsibility for establishing and maintaining SnowBe's information security management system to ensure the availability, integrity, and confidentiality of SnowBe's information. They are also responsible for the development and improvement of the company's information security posture.

IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts): are responsible for proper implementation of security requirements within the information technology resources when change occurs.

Management – Responsible for reviewing and complying with the Security and Awareness Training, completing the required annual PCI self-assessment (SAQ), completing the annual PCI training through Financial Management, requiring appropriate staff to complete the annual PCI training through Financial Management, and maintaining departmental Standard Operating Procedures (SPO) for PCI compliance and verify employees have an understanding of the procedures and their responsibilities.

Payment Card Handlers and Processors – Responsible for following the established cash receipts procedures for the appropriate funding source, following the Payment Card Processing Options, and using PCI Compliant Devices for all card transactions, and reviewing and complying with the the Security and Awareness Training.

PCI Compliance Committee – Responsible for monitoring the university's compliance with PCI DSS requirements, acting as a steering committee for PCI DSS, supporting PCI DSS compliance efforts, and reviewing the required annual SAQ self-assessment

Policy, Compliance and Internal Controls – Responsible for maintaining an inventory of all SnowBe departments that process payment card transactions using an approved merchant account or other compliant methods, providing and monitoring annual training that meets the PCI DSS requirements, coordinating the completion of the annual self-assessment documents (SAQs), collecting departmental PCI procedures as part of the annual SAQs, and evaluating compliance with PCI as part of scheduled cash handling reviews; this is a shared responsibility with Financial Management.

Security Assurance - Responsible for implementing and executing this policy.

Security Assurance Management (Code Owners) - Responsible for approving significant changes and exceptions to this policy

Security Compliance Team - Responsible for the continuous monitoring of change management procedures across the relevant systems through security control testing to ascertain adherence to this policy.

Security and Information Compliance Officers: are responsible for SnowBe's security programs, including risk management. They play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the information technology resources that support the company's mission and compliance needs.

SnowBe Leadership (including store managers) - Accountable for the effective implementation of this policy within their areas of managerial responsibility. They are also accountable for ensuring that information in their category is not put at undue risk. They will approve all use and sharing of information in their category, having considered the risks and benefits.

Technical System Owners, Business System Owners, and System Administrators - Responsible for ensuring the minimum requirements established by this policy are implemented in procedure and executed consistently.

Team Members - Responsible for following change management procedures in a way that aligns with this policy.

Section 5: Statement of Policies, Standards and Procedures

Policies

AC-2 SPA Security and Privacy Attributes

Provide the means to associate [Assignment: organization-defined types of security and privacy attributes] with [Assignment: organization-defined security and privacy attribute values] for information in storage, in process, and/or in transmission. Ensure that the attribute associations are made and retained with the information.

AC-16 AM Account Management Policy

The purpose of this policy is to establish a standard for the administration of computing accounts that facilitate access or changes to SnowBe Online data. An account, at minimum, consists of a user ID and a password; supplying account information will usually grant access to some set of services and resources. This policy establishes standards for issuing accounts, creating password values, and managing accounts.

AC-20 UES Use of External Systems

This policy applies to all employees, contractors, and third-party users who have access to SnowBe Online's systems and data and utilize external systems for business purposes. It covers a wide range of external systems, including cloud services, third-party applications, remote network connections, and software-as-a-service (SaaS) platforms. The policy also encompasses the responsibilities and obligations of all individuals interacting with external systems on behalf of SnowBe Online.

AC-21 IS Information Sharing

This policy applies to all employees, contractors, partners, and authorized third parties who have access to SnowBe Online's information assets and engage in information sharing activities. It encompasses both internal information sharing within the organization and external information sharing with trusted entities, such as business partners, customers, and regulatory authorities.

AC – LP1 Least Privilege Policy

Centralized access management is key to ensuring that authorized SnowBe Online employees have access to the correct data and systems at the correct level. SnowBe access controls are guided by the principle of least privilege and need-to-know.

CCM-1 Change Control Management Policy

The purpose of the Change Control Management Policy is to ensure that a standard set of minimum requirements are established for changes that are made to production systems and supporting infrastructure across the organization.
These requirements are meant to provide a level of consistency across how changes are managed from the initial change request through to production deployment.

PM-1 Patch Management Policy

The purpose of this policy is to enforce patch requirements for SnowBe-owned or managed IT Resources.

SC-1 Cryptographic Protection

Information is an asset and access to it must be managed with care to ensure that confidentiality, integrity, and availability are maintained. Encryption of information and devices helps mitigate the risk of unauthorized interception, disclosure, and access. SnowBe Online uses encryption to secure information and data while stored, processed, and handled, protect user credentials, and enable secure communications.
This policy outlines SnowBe's approach to cryptographic controls, and management, and provides the requirements and responsibilities to ensure information security and data governance objectives are met.

SC-7 Boundary Protection

The purpose of the SC-7 Boundary Protection Policy is to establish guidelines and controls for protecting SnowBe Online's network boundaries against unauthorized access, malicious activities, and data breaches. This policy aims to ensure the confidentiality, integrity, and availability of SnowBe's systems and data by implementing appropriate boundary protection measures.

SDLC- SDLC Policy

The purpose of the Systems Development Life Cycle (SDLC) Policy is to describe the requirements for developing and/or implementing new software and systems at SnowBe and to ensure that all development work is compliant as it relates to any and all regulatory, statutory, federal, and /or state guidelines.

SI-7 Software, Firmware, and Information Integrity

The purpose of this policy is to ensure the integrity and security of software, firmware, and information within SnowBe Online. It establishes guidelines and controls to protect against unauthorized access, modification, or corruption of software and firmware components, as well as ensuring the accuracy and reliability of information stored and processed within the organization's systems.

SM-1 Security Maturity Policy

This policy establishes SnowBe-wide strategies and responsibilities for protecting the confidentiality, integrity, and availability of the information assets that are accessed, managed, and/or controlled by the company. Information assets addressed by the policy include data, information systems, computers, network devices, as well as documents and verbally communicated information.

By implementing this policy, SnowBe will:

Establish a Company-wide information security framework to appropriately secure access to information resources and services;

Protect against unauthorized access to, use, or sharing of, sensitive information that could potentially result in harm to SnowBe or its employees

Protect against anticipated threats or hazards to the security of information assets;

Comply with federal, state, and local law, company policies, and agreements binding SnowBe that require the company to implement applicable security safeguards.

SP- AC1 Access Control Policy

The purpose of this policy is to establish the guidelines and procedures for controlling access to SnowBe Online systems and resources to ensure the confidentiality, integrity, and availability of information.

SP-AU1 Acceptable Use Policy
This policy is to outline the acceptable use of computer equipment and other electronic devices at. These rules are in place to protect the employee. Inappropriate use exposes cyber risks including virus attacks including ransomware, compromise of network systems and services, data breach, and legal issues

SP-IR1 Incident Response Policy

The purpose of this policy is to define the framework for effectively responding to and managing security incidents involving SnowBe Online systems and data. It outlines the roles, responsibilities, and procedures to detect, analyze, contain, eradicate, and recover from security incidents in a timely and efficient manner.

SP- PCI1 PCI Compliance Policy

This policy provides guidance about the importance of protecting payment card data and customer information. Failure to protect this information may result in financial loss for customers, suspension of credit card processing privileges, fines, and damage to the reputation of SnowBe online.

SP-PS1 Physical Security Policy

This policy establishes requirements for the management, control, monitoring, and removal of physical access to SnowBe facilities containing Information Technology (IT) Electronic Resources.

SC-28 Protection of Information at Rest

This policy applies to all data stored by all employees, contractors, consultants, temporary, and other workers at SnowBe Online, including all personnel affiliated with third parties conducting SnowBe Online business. All data covered by the scope of this policy will be classified as Protected data, Sensitive data, or public data.

SP-RA1 Risk Assessment Policy
The execution, development and implementation of remediation programs is the joint responsibility of Infosec and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Infosec Risk Assessment Team in the development of a remediation plan.

SP- SA&T1 Security Awareness and Training Policy

The purpose of this policy is to ensure that all SnowBe employees affiliates with access to company data, are taught Information Security Awareness in order to gain an understanding of the importance of securing said data. SnowBe Online seeks to establish a culture that ensures that all company data is secure.

SC – 8 Transmission Confidentiality and Integrity
This policy applies to all Information Systems and Information Resources owned or operated by or on behalf of SnowBe Online. All SnowBe Online-Related Persons with access to SnowBe Online Information or computers and systems operated or maintained on behalf of Snowbe Online are responsible for adhering to this policy.

SR-1 Component Disposal

Technology equipment often contains parts that cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs, and other storage media contain various kinds of SnowBe Online data, some of which are considered sensitive. To protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion but is still accessible until being overwritten by a new file.
Therefore, special tools must be used to securely erase data prior to equipment disposal. The purpose of this policy is to define the guidelines for the disposal of technology equipment and components owned by SnowBe.

Standards and Procedures

NAC-1 New Account Creation Procedure

The purpose of this policy is to establish a standard for the administration of computing accounts that facilitate access or changes to SnowBe Online information resources. An account, at minimum, consists of a user ID and a password. Supplying account information will usually grant access to some set of services and resources. This policy establishes guidelines for issuing and managing accounts.

Section 6: Exceptions/Exemptions

Requests for exceptions from SnowBe security controls, standards, or practices must be submitted in writing to the IT Department. At a minimum, each request shall have the following information completed by the requestor, or the request will not proceed:

Contact information on the requestor and authorized signer

The standard, practice, or controls from which an exception is desired Request type (i.e. Exception, Exemption)

Explanation of the Request Business Justification/Reason

The IT Department conducts a risk assessment on the request.

If needed, the IT Department will conduct a review of the assessment.

The IT Department documents the results of the risk assessment and will then accept or reject the request.

All requests that are granted must be reviewed and/or renewed annually

Section 7: Version History Table

Version	Date	Description
1.0	June 6, 2023	Creation of a Security Plan – first draft of Introduction, Scope, Definitions, Roles and Responsibilities, and Statemen of Policies, Standards, and Procedures.
2.0	June 12, 2023	Adding access controls
3.0	June 19, 2023	Updated Introduction, Scope, Definitions, Roles and Responsibilities, and Statemen of Policies, Standards, and Procedures.
4.0	October 22, 2023	Updated Definitions, and Statement of Policies, Standards, and Procedures.

Citations

2021-01 it physical security policy - uconn health. (n.d.-a). https://health.uconn.edu/policies/wp-content/uploads/sites/28/2021/03/2021-01-IT-Physical-Security-Policy.pdf

Access management policy. GitLab. (n.d.). https://about.gitlab.com/handbook/security/access- management-policy.html#purpose

Acceptable use policy - assets.contentstack.io. (n.d.-b). https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt207beda4b7c14d22/636f1a30e3836b0c88e8f0a8/Acceptable_Use_Policy.pdf

Acceptable use policy. University IT. (2021, November 10). https://tech.rochester.edu/policies/acceptable-use-policy/

Account management. – Policies And Procedures - Montclair State University. (n.d.). https://www.montclair.edu/policies/all-policies/account-management-policy/

Change management policy. GitLab. (n.d.). https://about.gitlab.com/handbook/security/change-management-policy.html#:~:text=The%20purpose%20of%20the%20Change,supporting%20infrastructure%2 0across%20the%20organization. https://www.cisecurity.org/

Create your login.gov account. Login.gov. (n.d.). https://www.login.gov/help/get-started/create- your-account/

Glossary of cyber security terms. Glossary of Security Terms | SANS Institute. (n.d.-a). https://www.sans.org/security-resources/glossary-of-terms/

GP-001.02 – security exceptions and exemptions to its standards practices & controls. UT System Policies. (2022, June 23). https://policy.tennessee.edu/procedure/gp-001-02-security- exceptions-and-exemptions-to-its-standards-practices-controls/ https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release- search#/control?version=5.1&number=AC-16

https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures- and-guidelines/data-at-rest-policy/

https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies- standards-and-guidelines/data-encryption-standard

https://policy.arizona.edu/information-technology/network-server-and-transmission-security- policy

Information security awareness policy. Connecticut College. (n.d.). https://www.conncoll.edu/information-services/policies/information-security-awareness-policy/

Information security policy - university of michigan. (n.d.). https://spg.umich.edu/sites/default/files/601x27.pdf

It security plan. IT Security Plan | IT Security | Iowa State University. (n.d.). https://security.it.iastate.edu/policies/it-security-plan

LSI Independent College Risk Assessment Policy and procedures ... - lsi.edu. (n.d.-c). https://www.lsi.edu/pdfs/college/LSI%20Risk%20Assessment%20Policy%202021-2022.pdf

Payment card industry (PCI) compliance policy. Administrative Services Gateway – University at Buffalo. (2021, January 13). https://www.buffalo.edu/administrative-services/policy1/ub- policy-lib/pci-compliance.html

Privileged access policy - university of Cincinnati. (n.d.-d). https://www.uc.edu/content/dam/uc/infosec/docs/policies/Privileged_Access_Policy_9.1.14.pdf

Risk assessment policy - assets.contentstack.io. (n.d.-c). https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt16603a027193d8b9/5e9e0685f92340115007214d/risk_assessment_policy.pdf https://www.sans.org/

Security and privacy attributes - CSF tools. CSF Tools - The Cybersecurity Framework for Humans. (2021, May 29). https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-16/

Systems development life cycle (SDLC) policy. Systems Development Life Cycle (SDLC) Policy | Policy Library. (2009, December 1). https://policy.ku.edu/IT/systems-development-life-cycle-policy

Systems development life cycle (SDLC) standard. Systems Development Life Cycle (SDLC) Standard | Policy Library. (2009, December 1). https://policy.ku.edu/IT/systems-development-life-cycle-standard

Technology equipment disposal policy. Technology Equipment Disposal Policy - Staff.Wiki. (n.d.). https://staff.wiki/486.page.technology_equipment_disposal_policy.kb.aspx

University, F. (n.d.). *Patch Management policy*. Fordham University. https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/patch-management-policy/

University of Aberdeen Cryptographic policy 1. (n.d.). https://www.abdn.ac.uk/staffnet/documents/policy-zone-information-policies/Cryptographic%20Policy.pdf

What is deprovisioning?. SailPoint. (2021, July 7). https://www.sailpoint.com/identity- library/what-is deprovisioning/#:~:text=Deprovisioning%20is%20the%20act%20of,for%20users%20in%20a% 20system.

What is provisioning?. Red Hat - We make open source technologies for the enterprise. (n.d.). https://www.redhat.com/en/topics/automation/what-is-provisioning#:~:text=Provisioning%20is%20the%20process%20of,%2C%20edge%20devices%2C%20and%20more.

What is user access rights. technology. (2021, March 16). https://quest-technology- group.com/academy/what-is-user-access-rights#:~:text=Access%20rights%20are%20the%20permissions,computers%2C%20and%20o nline%20file%20storage.