SC-13 SNOWBE ONLINE Cryptographic Protection Policy

Your name: Phillip White

Cryptographic Protection

Version 1.0

DATE: November 12, 2023

Table of Contents

Purpose

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 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 control management and provides the requirements and responsibilities to ensure information, security, and data governance objectives are met.

Scope

- All individuals, including staff, contractors, and visitors, who have access to SnowBe digital services, information, login credentials, and technologies.
- All facilities, technologies, and services that are used to process SnowBe's information.
- All information processed, accessed, manipulated, or stored by SnowBe.
- Internal and external processes that are used to store, transfer, or process SnowBe's information.
- External parties and suppliers that provide information storage, hosted systems, transferal, or processing services to SnowBe.

Definitions

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

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.

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.

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.

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

File encryption: A method that encrypts individual files.

Plaintext: Unencrypted data

Roles & Responsibilities

Chief Information Officer (CIO):
The Office of the Chief Information Officer has overall responsibility for the security of SnowBe's information technologies. Implementation of security policies is delegated throughout SnowBe to various SnowBe services; departments, and other units; and to individual users of SnowBe IT resources.

Director of Information Security:
This role is responsible for ensuring various aspects of SnowBe's cyber and information security:

- Ensuring that SnowBe's staff, policies, processes, practices, and technologies proactively protect, shield, and defend the organization from cyber threats, and prevent the occurrence and recurrence of cybersecurity incidents commensurate with the organization's risk tolerance.
- Ensuring that SnowBe's staff, policies, processes, practices, and technologies monitor ongoing operations and actively hunt for and detect adversaries and report instances of suspicious and unauthorized events as expeditiously as possible.
- Ensuring that SnowBe's staff, policies, processes, practices, and technologies are rapidly deployed to return assets to normal operations as soon as possible.
- Ensuring that SnowBe's leadership, staff, policies, processes, practices, and technologies provide ongoing oversight, management, performance measurement, and course correction of all cybersecurity activities.

IT Security and Policies Team:
IT security and policies team is responsible for ensuring the security of the provided IT services. The security and policy team must make sure that all intellectual property and proprietary information are protected. This role is responsible for taking all necessary precautions to ensure the security of the services provided by SnowBe.

Data Steward:
SnowBe office represented by an executive officer. The data steward has policy-level and planning responsibilities for data owned by SnowBe in their functional areas. Data stewards, as a group, are responsible for recommending policies and establishing procedures and guidelines for SnowBe-wide data administration activities. Data stewards may delegate the implementation of SnowBe policies, standards, and guidelines to data custodians.

Data Custodian:
The data custodian is the individual or entity (including outsourced services) in possession or control of data and is responsible for safeguarding the data according to the policies and procedures established by the associated data steward. The appropriate level of protection is based on the SnowBe Data Classification policy and the Minimum Security Standards for Protected Data.

Data User:
The data user, synonymous with user, is the individual, automated application or process that is authorized by the data steward to create, enter, edit, and access data, in accordance with the data steward's policies and procedures. Users have a responsibility to:

- Maintain the security of passwords, personal identification numbers (PINs), authentication tokens, and certificates; and will be held accountable for any activities linked to their accounts.
- Manage all forms of authentication and security controls for information processing systems based on the Minimum-Security Standards for Protected Data.
- Use the data only for the purpose specified by the data steward.
- Comply with controls established by the data steward.
- Prevent disclosure of confidential or sensitive data.
- Report suspected security incidents that may have breached the confidentiality of data.

Departments, and Other Units:
Departments and other units are responsible for securing any information they create, manage, or store, and for any information, they acquire or access from other SnowBe systems (e.g., PCI data, personnel records, business information). This responsibility includes completing periodic risk assessments, developing, and implementing appropriate security practices, and complying with all aspects of this policy.

Policy

- Protecting data at rest - encrypting data while it is stored provides effective protection against unauthorized access and theft. Encryption must be used to protect SnowBe digital data at rest. Options for encryption of data at rest include:
    - Full disk encryption
    - File encryption
    - Application encryption
    - Database encryption

- All SnowBe-owned devices and storage systems must have full disk encryption enabled and, where possible, monitoring must be in place to ensure this continues to be enabled and effective.
- Protecting data in transit - encrypting data while in transit provides effective protection against unauthorized interception and access. Encryption must be used to protect SnowBe digital data in transit.
- Protecting data copied to external devices – all data copied to external or removable storage devices must be encrypted.
- Encryption must be implemented using approved methods and technologies. Encryption standards, algorithms, protocols, key length, and cipher suites must meet current acceptable standards as defined in the SnowBe standard. Systems, infrastructure, applications, and services must be configured to only accept connections that comply with this requirement.
- Unsupported ciphers, protocols, and algorithms must be disabled where possible. Superseded or insecure protocols and cipher suites should not be used unless there is an approved exception in place.
- Encryption algorithms and specific implementations of algorithms can contain vulnerabilities. The use of algorithms and encryption software must be monitored and managed through the vulnerability management process.
- Cryptographic keys must be generated, stored, and managed in a secure manner that prevents loss, theft, or compromise.
- Access to cryptographic keys must be restricted to authorized individuals.
- Cryptographic keys must be transmitted by reliable and secure methods to maintain confidentiality and integrity. Separate communication channels should be used for key and data transfer. Under no circumstances should the key and encrypted data be transferred together via the same medium.
- There must be procedures and controls in place for key or certificate revocation in the event of compromise or expiry.
- It is important to recognize that even with encryption in place there is residual risk to the confidentiality of data. Therefore, secure data handling procedures should always be followed for sensitive and confidential information even whilst that information is encrypted.

Exceptions/Exemptions

Exceptions:

- An exception is a deviation from a policy that is granted on a case-by-case basis. Exceptions may be granted for the following reasons:
    - A compelling business need that cannot be met without violating the policy.
    - A technical constraint that prevents compliance with the policy
    - A legal or regulatory requirement that conflicts with the policy.

Exemptions:

- An exemption is a blanket waiver from a policy that applies to a specific group of people, systems, or processes. Exemptions may be granted for the following reasons:
    - The group of people, systems, or processes is not subject to the risks that the policy is designed to mitigate.
    - The group of people, systems, or processes is already subject to equivalent or superior controls.
    - The cost of complying with the policy would outweigh the benefits.

Process for requesting an Exception or Exemption:

- To make a request, please submit a written (snail mail or email) request to the appropriate policy owner. The request should include the following information:
    - The specific policy that you are requesting an exception or exemption from.
    - The reason for the request.
    - The proposed alternative controls if any.
    - The duration of the exception or exemption.

Reviewing and Granting Exceptions or Exemptions:

- The policy owner will review the request and make a decision based on the following factors:
    - The severity of the risk that the policy is designed to mitigate.
    - The likelihood that the risk will materialize.
    - The impact of the risk if it materializes.
    - The effectiveness of the proposed alternative controls.
    - The cost of complying with the policy.

The policy owner may grant the exception or exemption, deny the request, or request additional information.

Documentation:

All exceptions and exemptions must be documented in writing and should include the following information:

- The specific policy that the exception or exemption applies to.
- The reason for the exception or exemption.
- The proposed alternative controls if any.
- The duration of the exception or exemption.
- The name of the person who granted the exception or exemption.

Review:

All exceptions and exemptions will be reviewed annually and revoked if they are no longer necessary.

Enforcement

Employees who violate SnowBe Online policies may be subject to disciplinary action, up to and including termination of employment. In addition, employees may be held personally liable for any damages caused by their violation of policy.

In addition to disciplinary action, employees who violate SnowBe Online policies may also face legal consequences. These consequences may include:

- Civil lawsuits
- Criminal prosecution
- Regulatory fines

Disclaimer:
This penalty clause is not intended to be a comprehensive list of all possible consequences of violating SnowBe Online policies. Employees are responsible for complying with all SnowBe Online policies and should consult with their supervisor or the Human Resources department if they have any questions.

Version History Table

Version #	Change/Implementation Date	Document Owner	Approved By	Description
1.0	November 12, 2023	P. White		Initial Draft

Citations

https://www.abdn.ac.uk/staffnet/documents/policy-zone-information-policies/Cryptographic%20Policy.pdf