SNOWBE ONLINE

Data Encryption Policy

Your name: Chris Stevens

Data Encryption Policy

Version # 1.0

DATE: 5-12-2025

Table of Contents

Purpose

This document provides the SnowBe Online community with the information required to effectively and efficiently plan, prepare and deploy encryption solutions in order to secure Legally/Contractually Restricted Information (Sensitive Data).

The focus is on providing a range of tools for the most common systems that are likely to be deployed in the SnowBe Online environments which store, transmit or process Sensitive Data.

When properly implemented, encryption provides an enhanced level of assurance that the data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception.

Scope

Where technically feasible, the Data Encryption Policy applies to all faculty or staff members, whether full-time or part-time, paid or unpaid, temporary or permanent, as well as all agents and representatives of SnowBe Online, including any third-party service provider providing services to SnowBe who create, use or otherwise access or interact with any SnowBe Online's Information or Company Information Resource.

Definitions

AES
Advanced Encryption Standard is cryptographic cipher that uses a block length of 128 bits and key lengths of 128, 192 or 256 bits to protect data.

Asymmetric Key
A form of encryption where keys come in pairs. What one key encrypts, only the other can decrypt. This is used in digital signatures and also in public-key cryptography such as PGP where you share your public key with anyone. The data is encrypted with your unshared private key and can be decrypted with your public key that you have shared. The public-key cannot encrypt any data it can only decrypt a message already encrypted with the paired private key.

Elliptical Curve Key
Is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

Encryption
The process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Encryption Key
A sequence of numbers used to encrypt or decrypt data.

Encryption Key Management
In Encryption it is the creation, distribution and maintenance of a secret key. It determines how secret keys are generated and made available to both parties.

Kerberos
Is a secure method for authenticating a request for a service from a computer by providing an encrypted master ticket, which is created on initial user logon to a Kerberos system.

PGP
Pretty Good Privacy (PGP) is a computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting and decrypting e-mails to increase the security of e-mail communications. It is also used to provide disk and file encryption.

RSA
Is an algorithm for public-key cryptography and is used for signing as well as encryption.

Secure Socket Layer (SSL)
Is a security protocol used to validate the identity of a Web site and to create an encrypted connection for sending sensitive data.

SSH
Secure shell is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

Symmetric Key
An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message (example DES).

SnowBe Information Resource
Any tool, device, equipment, or system used to create, collect, record, process, store, retrieve, display and transmit University Information, including but not limited to email, mainframes, servers, computers, laptops, personal digital assistants (PDA), telecommunication resources, fax machines, printers, file cabinets, software and embedded technology.

Roles & Responsibilities

All personnel employed by SnowBe Online are required to comply with this policy. Our company's leadership and management team are responsible for maintaining and enforcing the policies, standards and guidelines established within this document. Employees, contractors, vendors, service providers, partners, affiliates, and third parties are responsible for ensuring all actions are in accordance with our management policies and objectives.
With this Data Encryption Policy ALL users are required to sign our company's Acceptable Use Policy and acknowledge they understand and will abide by the standards and individual responsibilities it defines. All changes to the Acceptable Use Policy are communicated to all staff, contractors and other third parties in a timely fashion.

Policy

All Encryption must meet the following minimum requirements:

- Symmetric key lengths of at least 128 bit
- Asymmetric key lengths of at least 2048
- Elliptic Curve key lengths of at least 256 bit
- AES key lengths of at least 128 bit
- RSA key lengths of at least 2048
- Web server certificates TLSv1.2 (example secure web sites HTTPS)
- SSH version 2 (example network device administration)
- Kerberos (example windows server and connecting device)
- PGP – AES 128 bit (example whole disk, file, USB, and email encryption)
- PGP – Public Keys RSA 2048 (for example digital signatures and encrypted email).

The Information Security Officer must approve all Encryption technologies used on University Information Resources. Approved Encryption will be based on publicly proven algorithms and technologies. No other Encryption technology may be used.

Digital Certificates

- Public-facing Secure Socket Layer (SSL) services must use digital certificates issued by a trusted authority approved by the Information Security Officer or Chief Information Officer.
- Non-public facing SSL services may use self-signed digital certificates when used for management purposes.
-

Encryption Key Management

- Encryption Key Management procedures must ensure that authorized users can access and decrypt all encrypted data and comply with data retention requirements. (see Retention Records Policy)
- Encryption keys must have at least 2 approved authorized users who can access and decrypt the applicable encrypted information.
- All Encryption keys must be treated as Confidential Information and must be stored securely. (See Data Classification Policy)

Some data is subject to encryption standards by law. To the extent that such legal requirements are different or more specific than required under this Policy, the applicable legal requirements shall be followed. For example, any use of credit cardholder data must follow PCI-DSS encryption requirements (see PCI-DSS standards https://www.pcisecuritystandards.org).

Violation of Policy

The SnowBe Online reserves the right to monitor network traffic, perform random audits, and take other steps to ensure the integrity of its information and compliance with this Policy. Violations of this Policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this Policy may result in dismissal from the Company.

Exceptions/Exemptions

Exceptions to this plan must be approved by the Information Security Office, under the guidance of SnowBe's IT Director and/or IT Manager. All exceptions will be formally documented. Plan exceptions will be reviewed on a periodic basis for appropriateness. Please note that while requesting exceptions or exemptions has been made available to you, it does not guarantee approval.

SnowBe Online recognizes that, under certain circumstances, deviations from this Acceptable Use Policy may be necessary to support specific business needs or technical requirements. Exceptions or exemptions to this policy may be granted under the following conditions:

Risk Acceptance
In some rare cases, a business case for non-compliance can be established. In all such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a department manager and reviewed by IT Enterprise Security and IT Information Systems and approved by the IT Director and/or IT Management. Further details on the risk acceptance process can be obtained through the Enterprise IT Security Department.

Pre-Approval Required
All exceptions must be formally requested in writing and approved by the IT department and an authorized member of management. The request must clearly state the business justification, duration, and potential risks of the exception.

Documentation and Review
Approved exceptions will be documented and maintained by the IT department. All exceptions are subject to periodic review to ensure they remain valid and do not introduce unacceptable risks.

Temporary and Specific
Exceptions are granted on a temporary basis for clearly defined scopes and timeframes. They do not constitute a permanent change to the policy.

No Unauthorized Exceptions
Any deviation from this policy without documented approval is considered a violation and may result in disciplinary action, including suspension of access privileges.

Compliance Priority
Exceptions will not be approved if they compromise SnowBe Online's compliance with legal, regulatory, or security requirements.

Enforcement

Enforcement
SnowBe Online takes the enforcement of this (Policy name) seriously to protect its systems, data, and customers.

Violations of this policy, whether intentional or accidental, may result in disciplinary action, up to and including termination of employment, contract cancellation, and/or legal action.

The penalties will include the following components:

Monitoring and Auditing
SnowBe Online reserves the right to monitor, log, and audit all system and network activity to ensure compliance with this policy. Users should have no expectation of privacy when using company-owned systems or accessing company data.

Incident Investigation
Suspected policy violations will be investigated promptly by the IT department, Human Resources, and other relevant stakeholders. Users are expected to cooperate fully during any investigation.

Corrective Action
If a violation is confirmed, corrective actions will be taken based on the severity and nature of the breach. This may include revocation of access, mandatory training, written warnings, or other disciplinary measures as outlined in the employee handbook.

Legal Consequences
Activities that are illegal under local, state, or federal law may be reported to the appropriate authorities. This includes unauthorized access, data breaches, or misuse of customer financial information.

Appeals Process
Individuals who believe they were unfairly penalized for a policy violation may appeal the decision to management or HR following internal dispute resolution procedures.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	5-12-2025	SnowBe Online	IT Management	Policy Creation

Citations

Bowie State University
https://www.bowiestate.edu/files/resources/information-security-public.pdf
Exceptions/Exemptions

ChatGPT
https://chatgpt.com/c/681bc793-d1dc-800b-a676-cb7b3cf2678d
Exceptions/Exemptions, but as a group we revised the verbiage.

Policy Template
https://www.sans.org/information-security-policy/
Exceptions/Exemptions

Northwestern
https://www.it.northwestern.edu/about/policies/dataencryption.html
Purpose

ITS Information Security
https://wikis.suffolk.edu/display/ITSEC/Encryption+Policy
Definitions, Policy

National Cybersecurity Society
https://nationalcybersecuritysociety.org/wp-content/uploads/2019/10/Encryption-Policy-Template-FINAL.pdf
Roles and Responsibilities