SNOWBE ONLINE

Endpoint Security

POLICY

Your name: Chris Stevens

End Point Security

Version # 1.0

DATE: 5-12-2025

Table of Contents

Purpose

This Endpoint Security policy establishes minimum security requirements for protecting SnowBe Online systems, including operating systems and endpoint computing systems. This policy outlines the minimum system, software, and process protections that must be applied for all SnowBe Online-owned Endpoint Devices (e.g. laptops, desktop, servers, mobile devices, etc.) as well as all other Endpoint Devices.

Endpoint Devices that contain or process Company Data are a fundamental part of the SnowBe Online information technology landscape that includes internally managed information technology resources as well as externally managed resources in the cloud or at other third-party vendor locations. Endpoint Devices are an important source of connecting end users to Company Data via networks and systems and are a major source of how vulnerabilities and other information security threats are introduced into SnowBe Online's information technology landscape. Compliance with this Endpoint Standard helps ensure the protection, confidentiality, integrity, and availability of SnowBe Online's systems and Company Data.

Departments and units may impose more, but not less, stringent requirements and standards as they deem appropriate or necessary based on applicable laws, regulations, or contracts.

Scope

This Policy applies to all SnowBe Online employees, as well as other users of the network infrastructure, including independent contractors or temp employees who may be given access on a temporary basis to SnowBe Online's systems.

The audience of this Endpoint Standard is any member of the SnowBe Online community (including vendors, contractors, suppliers, visiting faculty, etc.) who use, manage, or maintain an Endpoint Device that accesses Institutional Data.

If a department or business unit determines that use of a Personally-Owned Endpoint Device is required for SnowBe Online Business, it is the responsibility of the department or business unit to ensure protections equivalent to those outlined in this Endpoint Standard are applied. Departments or business units can contact SnowBe Online's Information Security Office with questions about the security of Personally-Owned Endpoint Devices.

Definitions

Endpoint Devices
Endpoint Devices are physical or virtual machines that have the ability to collect, store, and/or process information. Some examples of Endpoint Devices include, but are not limited to, desktop or laptop computers, mobile phones, tablets, virtual machines, embedded devices, and servers. Internet-of-Things (IoT) devices, such as "smart" equipment (cameras, lighting, appliances, speakers, or thermostats) are also Endpoint Devices.

Information and Communication Technology (ICT
An umbrella term used to describe all information and communication technologies, that includes, but is not limited to, the Internet, wireless technologies, software, systems, applications, public/private/hybrid cloud, computers, social network, as well as other media applications and services.

Information Security Advisory Committee (ISAC)
A SnowBe-wide technology governance group that is responsible for monitoring the security maturity and controls of SnowBe Online and providing approval for all security vulnerability exceptions that pose a significant or high risk.

Information Security Governance, Risk, Compliance
A combination of three approaches that organizations use to demonstrate compliance with international standards, global rules, laws, and state regulations. Governance, risk management, compliance (GRC) is often implemented by companies that are growing globally to maintain consistent policies, processes, and procedures across all parts of the organization.

Company Data
All data that SnowBe Online is responsible and accountable for protecting. This data includes, but is not limited to, data SnowBe owns, collects, intellectual property owned by faculty or others, staff data, employee data, faculty data, research data, personal information, vendor and contractor data, and data that SnowBe Online shares or provides to third parties for storage, processing, and analysis.

SnowBe Online-owned Systems or Devices
ICT (including, without limitation, laptops, desktops, tablets, mobile phones, and IoT devices) that are the responsibility of the University to account for and provide appropriate safeguards. This includes ICT purchased (either directly or by reimbursement) from a SnowBe chart of accounts, or devices with documented ownership or responsibility transferred to the SnowBe Online from another Company or organization.

Personal or Personally-owned Devices
ICT (including, without limitation, laptops, desktops, tablets, mobile phones, and IoT devices) that are wholly owned by an employee, or affiliate of SnowBe Online.

SnowBe Online Business
Any activity carried out under the auspices of SnowBe Online and in furtherance of the SnowBe Online’s mission.

SnowBe Online Network
The SnowBe Online Network is the infrastructure and equipment that connects information and communication technology (ICT) to enable the exchange of data and information at SnowBe. This includes connections that are limited to within the company as well as the broader Internet. The SnowBe Online Network includes both physical wired (wall jacks, wiring, routers, switches, etc.) and wireless network components, including ad-hoc wireless networks. The SnowBe Online Network also includes connections provided by a third-party telecommunications provider but managed by SnowBe IT, or network paths over hardware or software (such as VPN, site-to-site tunnel, etc.) by which a user or ICT device receives a SnowBe-managed IP address, telephone number, or other SnowBe Online-owned network descriptor.

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

The objective of this policy is to protect and preserve an environment through the responsible use of Information Technology (IT) resources, and to ensure that employees of the SnowBe Online have access to reliable and robust IT resources that are safe from unauthorized or malicious use. This policy applies to SnowBe Online-Owned Technology Resources, this includes, but is not limited to, desktops, workstations, laptops, and mobile storage devices purchased from all sources of SnowBe Online funds. This policy also applies to personally purchased devices used for SnowBe Online's business purposes.

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

USC University of Southern California
https://policy.usc.edu/wp-content/uploads/2022/12/P07-Endpoint-Security-v1.4_10.2022.pdf
Purpose, Scope

Northwestern
https://www.it.northwestern.edu/about/policies/endpoint-security.html
Scope, Definitions

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