SNOWBE ONLINE Policy# AC-17
Remote Work Security

Humberto Gonzalez

Version # 1.0

DATE: July 5, 2024

Table of Contents

Purpose

This policy defines the requirements for secure access to SnowBe Online information, networks and computing resources by authorized remote workers. This arrangement is also known as “teleworking” or “remote working”.

Scope

This policy applies to all SnowBe Online employees and Third-Party contractors with remote access to information systems and networks.

Definitions

Confidential Information (Sensitive Information)– Any SnowBe Online information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by SnowBe Online from a Third-Party under a non-disclosure agreement.

Information Asset– Any SnowBe Online data in any form that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and Third-Party data.

Information System– Any SnowBe Online equipment, applications or systems used to manage, process, or store SnowBe Online data. This includes, but is not limited to, information systems managed by third-parties.

Mobile Computing Devices– Mobile computing assets include, but are not limited to laptops, notebooks, tablets, cell phones, and remote desktop computers. It also includes all portable storage media, including flash drives, smart cards, tokens, etc.

Password– An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

Third-Party– Any non-employee of SnowBe Online who is contractually bound to provide some form of service to SnowBe Online.

User– Any SnowBe Online employee or Third-Party who has been authorized to access any SnowBe Online electronic information resource.

Roles & Responsibilities

- Employees: Ensure their remote work environment is secure, and follow company policies.

- IT Department: Manages and monitors remote access systems, ensures a secure remote working environment is in place.

- Senior Management/Executive Team: Provides necessary tools and resources for secure remote work.

Policy

All remote access to SnowBe Online's systems must be safeguarded. Employees must ensure their home networks are secure and avoid using public Wi-Fi for accessing company resources.

Required Approval

- **Remote Working Privileges–** All employees working at home or at alternative sites must be specifically granted this privilege by the employee's manager or a member of the Information Technology Department.

- **Remote Working Agreement–** All SnowBe Online employees who are approved to work from remote locations must first sign an agreement to abide by all SnowBe Online remote worker policies, procedures and standards. The agreement should be reviewed and signed annually.

Compliance Requirements

- **Software License Restrictions–** Remote workers must follow software licensing restrictions and agreements on all software used to process Company information at alternative work sites.

- **Remote Working Information Security Policies–** Remote workers must follow SnowBe Online information security policies at remote work sites, including the Acceptable Use of Assets Policy.

Information Systems Security

- **Approved Remote Worker Equipment–** Employees working on SnowBe Online business at alternative work sites must use SnowBe Online provided computer and network equipment unless other devices have been approved by the IT Department.

- **Personally-Owned Information systems–** Remote workers must not use their own mobile computing devices, computers, computer peripherals, or computer software for SnowBe Online teleworking business without prior authorization from their supervisor.

- **Malware Protection Software–** All systems that access SnowBe Online networks remotely must have an anti-malware (anti-virus) package approved by the IT Department continually running.

- **Advanced Endpoint Protection–** All systems that access SnowBe Online networks remotely must have an endpoint protection software package installed that protects the system from advances threats.

- **Setting Date and Time–** Remote workers must diligently keep their remote computers' internal clocks synchronized to the actual date and time.

Remote Access Control

- **Access Control System–** Remote workers must not use a remote computer for SnowBe Online business activities unless this same computer runs an access control system approved by the IT Department.

- **Remote Access to Networks–** All remote access to SnowBe Online networks must be made through approved Remote Access points that are controlled by the Information Technology Department.

- **Session Logout–** After a remote worker has completed a remote session with SnowBe Online computers, the worker must log off and then disconnect, rather than simply disconnecting. Workers using remote communications facilities must wait until they receive a confirmation of their log off command from the remotely connected SnowBe Online machine before they leave the computer they are using.

- **Screen Positioning–** The display screens for all systems used to handle SnowBe Online sensitive information must be positioned such that they cannot be readily viewed by unauthorized persons through a window, over a shoulder, or by similar means.

- **Sharing Access and Systems Prohibited–** Remote workers must not share dynamic password token cards, smart cards, fixed passwords, or any other access devices or parameters with anyone without prior approval from the IT Department. This means that a remote computer used for SnowBe Online business must be used exclusively by the telecommuter. Family members, friends, and others must not be permitted to use this machine.

Alternative Work Sites

- **Alternative Work-Site Requirements**– Before a remote working (telecommuting) arrangement can begin, the worker's supervisor or manager must be satisfied that an alternative work-site is appropriate for the SnowBe Online work performed by the involved worker.

- **Separate Room or Workspace–** Whenever possible, remote working must be done in a separate room or workspace that can be locked or secured from the rest of the house or co-working space.

- **Inspections of Remote Working Environments–** SnowBe Online maintains the right to conduct inspections of teleworker offices with one or more days advance notice.

- **Remote Working Environmental Controls–** Equipment should be located and/or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

- **Lockable, Burglar-Resistant Furniture–** All workers who must keep sensitive SnowBe Online information and mobile devices at their homes to perform their work, must receive from SnowBe Online —or otherwise provide—approved lockable cabinets or desks for the proper storage of this information.

Data Protection

- **Encryption and Boot Protection–** All computers used for remote working (including portables, laptops, notebooks, and other transportable computers) which contain sensitive (Confidential or Secret) SnowBe Online information must consistently employ both hard disk encryption for all data files and boot protection through a password. These two essential controls must be provided through software or hardware systems approved by the IT Department.

Backup and Media Storage

- **Backup Procedures–** Remote workers are responsible for ensuring that their remote systems are backed up on a periodic basis, either automatically through the network or remotely with USB drives or similar equipment. If network backup is not available or feasible, SnowBe Online will provide telecommuters with local backup equipment.

- **Backup Media Storage–** If backups are made locally, telecommuting workers must store copies of these same backups at a secure location away from the remote working site at least every two weeks. If these backups contain sensitive information, the backups must be encrypted using software approved by the IT Department.

- **Sensitive Media Marking and Storage–** When sensitive information is written external storage media (external drives, CD-RW, USB drive, etc.), the media must be externally marked with the highest relevant sensitivity classification. Unless encrypted, when not in use, this media must be stored in heavy locked furniture. Smart cards and tamper-resistant security modules are an exception to this rule.

Remote System Management

- **Changes to Configurations and Software–** On SnowBe Online supplied computer hardware, workers must not change the operating system configuration or install new software. If such changes are required, they must be performed by Help Desk personnel with remote system maintenance software.

- **Changes to Hardware–** Remote working computer equipment supplied by SnowBe Online must not be altered or added to in any way without prior knowledge and authorization from the Help Desk.

Information Disposal

- **SnowBe Online Property at Alternative Work Sites–** The security of SnowBe Online property at an alternative work site is just as important as it is at the central office. At alternative work sites, reasonable and prudent precautions must be taken to protect SnowBe Online hardware, software, and information from theft, damage, and misuse.

- **Provision of Secure Containers–** Workers who must keep Secret or Confidential SnowBe Online information at their homes in order to do their work must have safes or lockable heavy furniture for the proper storage of this information. If these workers do not have such furniture or safes, SnowBe Online will loan these items to the telecommuting workers.

- **Shredders–** Remote workers must have or be provided with a shredder to appropriately dispose of printed versions of sensitive information. Shredders that make strips of paper are not acceptable for the disposal of SnowBe Online sensitive material. Acceptable shredders make confetti or other small particles.

- **Paper Records Disposal–** All printed copies of sensitive SnowBe Online information must be shredded for disposal. Telecommuting workers on the road must not throw away SnowBe Online sensitive information in hotel wastebaskets or other publicly-accessible trash containers. Sensitive information must be retained until it can be shredded, or destroyed with other approved methods.

System Ownership and Return

- **Return of Property–** If SnowBe Online supplied a telecommuter with software, hardware, furniture, information or other materials to perform SnowBe Online business remotely, all such items must be promptly returned to SnowBe Online when a telecommuter separates from SnowBe Online, or when so requested by the telecommuter’s manager.

- **Liability for SnowBe Online Property–** If SnowBe Online supplied a telecommuter with software, hardware, furniture, information or other materials to perform SnowBe Online business remotely, SnowBe Online assumes all risks of loss or damage to these items unless such loss or damage occurs due to the telecommuter’s negligence. SnowBe Online expressly disclaims any responsibility for loss or damage to persons or property caused by, or arising out of the usage of such items.

Exceptions/Exemptions

In circumstances where regular security standards cannot be followed, exceptions or exemptions may be requested. To request an exception or exemption, the requester must send a formal written request to the IT department, outlining the precise security protocol that cannot be followed and the justification for the request. The request should include a reason for why the exception or exemption is required, the potential impact on security, and any proposed compensatory controls. The Chief Information Officer (CIO) or a designated senior IT executive has the power to approve or reject such requests. Approved exceptions or prohibitions will be provided for a brief period not exceeding one year unless otherwise justified. The requester must make certain that the exception or exemption is reviewed and re-evaluated before the end of the permitted term.

Enforcement

All SnowBe Online employees, contractors, and third-party entities must comply with this security policy. Failure to follow the policies and procedures outlined will result in disciplinary action, which may include verbal or written warnings for minor infractions, temporary suspension from duty for repeated or serious violations, and termination of employment for severe or repeated noncompliance. If noncompliance results in legal consequences or financial loss for SnowBe Online, the company has the right to take legal action. Contractors and third-party entities that violate this security strategy may face contract termination and legal action, depending on the severity of the breach. All disciplinary actions will be carried out under SnowBe Online policy and any applicable labor laws. Each individual must understand and follow security policies to protect the company's information assets.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	07/05/2024	Humberto Gonzalez	TBD	Initial Version

Citations

Remote Work Security Policy- Sample Remote Working security policy (hubspot.net)

Exceptions/Exemptions- Sample Detailed Security Policy (bowiestate.edu)

Roles & Responsibilities- Sample Detailed Security Policy (bowiestate.edu)

Enforcement- Sample Detailed Security Policy (bowiestate.edu)