SNOWBE ONLINE SP-3
BACKUP POLICY

Your name: Jacob Barrera Section 01

SP-3 Backup Policy

Version #1

DATE: 12/4/2024

Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 3

POLICY 4

EXCEPTIONS/EXEMPTIONS 5

ENFORCEMENT 6

VERSION HISTORY TABLE 6

CITATIONS 7

Purpose

The purpose of this data backup plan is to ensure that SnowBe Online can safely and securely back up mission-critical data, systems, databases, and other technology so that it will be available in the event of a disruption affecting business operations. This plan aims to minimize operational disruptions and allow for rapid recovery when incidents occur. It contains specific procedures for full and incremental backups, data and document retention policies, storage and security measures, and responsibilities for managing backups. All SnowBe Online locations are expected to implement these data backup measures to maintain business continuity and protect critical information.

Scope

This policy applies to the entire SnowBe Online community, including all employees, contractors, volunteers, and guests who have access to SnowBe Online information technology resources. It encompasses both online and in-person interactions. The assets covered by this plan include data, images, text, and software stored on various media such as hardware, paper, or other storage devices.

Definitions

Access Control: The process of controlling access to systems, networks, and information based on business and security requirements.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Control Activities: The policies, procedures, techniques, and mechanisms that help ensure management's response to reduce risks identified during the risk assessment process is carried out.

Encryption: The process of converting information so that it is humanly unreadable except by someone who knows how to decrypt it.

Information Assets: Definable pieces of information in any form, recorded or stored on any media that is recognized as valuable to the organization.

Integrity: Guarding against improper information modification or destruction, ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Risk Assessment: A process to determine what information technology resources require protection and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability.

Roles & Responsibilities

Chief Information Security Officer (CISO)
- Lead the company's security efforts and make sure they meet business and legal requirements.
- Approve security policies and handle major security issues.
- Report on security risks and incidents to the leadership team.

Department Managers
- Approve employee access based on job needs.
- Let the IT Department know if someone's role changes or they leave the company.
- Make sure their teams follow the security rules.

Employees
- Follow security rules and training.
- Use strong passwords and keep accounts private.
- Report anything suspicious or unusual to IT.
- Keep company devices secure and use them responsibly.

IT Department
- Set up and manage security tools like firewalls, antivirus, and encryption.
- Control and monitor access to company systems and data.
- Fix security issues and keep systems updated.
- Watch for threats and respond quickly to security problems.

Security Team
- Check for risks and find ways to improve security.
- Keep an eye on the network for unusual activity.
- Plan and test how the company will respond to security incidents.
- Train employees to stay safe online.

Technical Consultant
- Employs controls using the NIST 800-53 framework and presents security advancement suggestions.

Third-Party Vendors
- Follow SnowBe Online's security rules and agreements.
- Use company systems only for approved tasks.
- Report any security issues immediately.

Policy

Full and incremental backups protect and preserve corporate network information and should be performed on a regular basis for system logs and technical documents that are not easily replaced, have a high replacement cost, or are considered critical. Backup media should be stored in a secure, geographically separate location from the original and isolated from environmental hazards. Backup network components, cabling and connectors, power supplies, spare parts and relevant documentation should be stored in a secure area on-site as well as at other corporate locations.

Data and document retention policies are established to specify what records must be retained and for how long. All departments are responsible for specifying their data management, data retention, data destruction and overall records management requirements.

IT Technical Support follows these standards for data backup and archiving:

System Databases

- A copy of the most current mission-critical databases must be made at least twice per month, or based on frequency of changes made.
- Backups must be stored off-site.
- The lead data administrator is responsible for this activity.

Mission-Critical Data

- Current mission-critical data and databases must be backed up according to the established recovery point objectives (RPOs), and must be mirrored or replicated to secure backup locations within the RPO time frames.
- Backups must be stored off-site at one or more secure cloud locations or at alternate company data centers or offices, or a combination of these.
- The lead data administrator is responsible for this activity.

Non-Mission-Critical Data

- Current non-mission-critical data and databases must be backed up according to the established RPOs, and can be mirrored or replicated to secure backup locations within the RPO time frames.
- Alternatively, copies of current data and databases must be made at least twice per week, or based on RPO metrics or the frequency of changes made.

- Backups may be stored on-site in secure storage facilities, or stored off-site at one or more secure cloud locations or at alternate company data centers or offices, or a combination of these.
- The data administration team is responsible for this activity.

Backup media are stored at locations that are secure, isolated from environmental hazards, and geographically separate from the location housing network components.

Off-site Storage Procedures

- Tapes and disks, and other suitable media are stored in environmentally secure facilities.
- Tape or disk rotation occurs on a regular schedule coordinated with the storage vendor.
- Access to backup databases and other data is tested annually.

Tapes (if used)

- Tapes greater than three years old are destroyed every six months.
- Tapes less than three years old must be stored locally off-site.
- The system supervisor is responsible for the transition cycle of tapes.

Exceptions/Exemptions

Exceptions and exemptions to SnowBe Online's security policies are granted on a case-by-case basis and are not guaranteed. Each request will be carefully evaluated to ensure it aligns with the company's overall risk management strategy and compliance requirements. Approved exceptions or exemptions must not create unacceptable security risks or regulatory violations and will be subject to regular review.

1. **How to Request an Exception or Exemption**
    - Submit a written request detailing the policy or control in question, the reason for the request, proposed mitigations, and the requested duration via the designated request platform (e.g., Service Desk or email to IT Security Team).

2. **Why an Exception or Exemption is Requested**

    - Provide a clear justification, including specific business, technical, or operational reasons that make adherence to the policy impractical or detrimental.

3. **Who Can Approve an Exception or Exemption**

    - Exceptions or exemptions must be approved by the IT Director or IT Manager. In some cases, approval may also require input from the Risk Management or Compliance team.

4. **How Long the Exception or Exemption Will Be in Place**

    - Specify the duration of the exception or exemption, including an expiration date. Temporary exceptions will be reassessed before renewal or termination. Permanent exemptions must undergo periodic review to ensure continued relevance and safety.

Enforcement

All individuals accessing Company data at SnowBe are required to comply with international, federal, and state laws, as well as Company policies and procedures regarding the security of highly sensitive data. Any Company employee, non-employed individual, vendor, consultant, or contractor with access to Company data who engages in unauthorized use, disclosure, alteration, or destruction of data is in violation of this policy and will be subject to appropriate disciplinary action. This may include termination of employment, removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1	12/4/2024	Jacob Barrera	Jacob Barrera	Created Backup Policy

Citations

https://frsecure.com/physical-security-policy-template/

https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fcommunity.trustcloud.ai%2FkbuPFACeFReXReB%2Fuploads%2F2022%2F10%2FData-Backup-Plan-Template.docx&wdOrigin=BROWSELINK