SNOWBE ONLINE Policy SP-2

Data Security Policy

Your name: Phillip White

Data Security - Version 1.0

DATE: October 27, 2023

Data Security – V 1.0
Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document owner: Phillip White
DATE: October 27, 2023

Table of Contents

Purpose

This Data Security Policy establishes the guidelines and procedures for protecting the confidentiality, integrity, and availability of all data within the organization. It aims to safeguard sensitive information from unauthorized access, modification, disclosure, or destruction, ensuring compliance with applicable data protection regulations and industry standards.

Scope

This policy applies to all employees, contractors, and other individuals who access, process, or store the organization's data, regardless of its format or location. It encompasses all types of data, including but not limited to:

- Customer data
- Employee data
- Financial data
- Intellectual property
- Confidential business information

Definitions

Confidentiality: The protection of data from unauthorized access.
Data Access Control: The process of restricting access to data to authorized individuals.
Data Backup: The process of creating a copy of data for recovery in the event of data loss.
Data Breach: A security incident involving the unauthorized access, modification, disclosure, or destruction of sensitive data.
Data Classification: The process of identifying and classifying data based on its sensitivity and potential impact if compromised.
Data Disposal: The process of securely disposing of data when it is no longer needed.
Data Encryption: The process of converting data into an unreadable format to protect it from unauthorized access.
Data Integrity: The assurance that data is accurate, complete, and consistent.
Data Recovery: The process of restoring data from a backup after data loss.
Incident Response Plan: A documented plan for responding to data breaches and other security incidents.
Least Privilege: The principle of granting users only the access and permissions they need to perform their job duties.
Physical Security: The measures taken to protect physical devices containing sensitive data from theft or unauthorized access.
Sensitive Data: Data that could cause harm to the organization or its individuals if compromised.
Cybersecurity Awareness: The understanding of cybersecurity threats and best practices for protecting data.

Roles & Responsibilities

Data Owner:

- The data owner is responsible for the overall security of their data, including its classification, access control, and disposal.

Data Custodian:

- The data custodian is responsible for the day-to-day management of the data, including its storage, backup, and recovery.

IT Department:

- The IT department is responsible for implementing and maintaining the organization's data security infrastructure and controls.

All Employees:

- All employees are responsible for complying with this Data Security Policy and for protecting the organization's data from unauthorized access, modification, disclosure, or destruction.

Policy

1. **Data Classification:** All data must be classified according to its sensitivity and potential impact if compromised. Classification levels include:
    - **Public:** Data that is publicly available and poses no risk if disclosed.
    - **Internal:** Data intended for internal use only, but not considered sensitive.
    - **Confidential:** Sensitive data that could cause harm if disclosed or modified.
    - **Restricted:** Highly sensitive data that could cause significant harm if compromised.
2. **Data Access Control:** Access to data must be restricted based on the principle of least privilege. Only authorized individuals with a legitimate business need should have access to specific data sets.
3. **Data Encryption:** Sensitive data must be encrypted at rest and in transit to protect it from unauthorized access or interception.
4. **Data Backup and Recovery:** Regular backups of all data must be performed to ensure its availability in case of system failures or cyberattacks.
5. **Data Breach Response:** A documented incident response plan must be in place to address data breaches promptly and effectively.
6. **Data Security Awareness and Training:** Employees and relevant personnel must receive regular training on data security policies, procedures, and best practices.
7. **Data Security Audits and Reviews:** Periodic audits and reviews of data security practices must be conducted to identify and address potential vulnerabilities.
8. **Data Disposal:** When data is no longer needed, it must be securely disposed of to prevent unauthorized access or reconstruction.

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	October 27, 2023	P. White		Initial Data Security policy draft completed

Citations

https://g.co/bard/share/469874f28b78