SNOWBE ONLINE SECURITY PLAN

Name: Lunick Francois

Version: 1.0
Date: 09/29/2024

Table of Contents

Section 1: Introduction

The purpose of this security plan is to outline the security policies, standards, and procedures in place at SnowBe Online to make sure of the protection of company assets, customer data, and system integrity.

Section 2: Scope

This plan applies to all employees, contractors, third-party service providers, and systems within SnowBe Online, including the company's websites, cloud services, and physical infrastructure.

Section 3: Definitions

- **System Development Life Cycle**: A methodology for developing, deploying, and maintaining systems.
- **Patch**: An update designed to fix vulnerabilities or improve functionality in existing software.
- **Security Maturity**: The level of security processes which are developed and integrated within the organization.
- **Threat Modeling**: The process of identifying potential security threats and developing strategies to lower them.

Section 4: Roles & Responsibilities

- **Chief Information Security Officer (CISO)**: Responsible for overseeing the implementation of security policies.
- **System Administrators**: Implement security controls and apply patches in line with established policies.
- **IT Security Manage**r: Coordinates patch management, vulnerability assessments, and security maturity assessments.
- **Employees/Contractors**: Follow security policies and report any potential vulnerabilities.

Section 5: Statement of Policies, Standards and Procedures

Policies

System Development Life Cycle Policy

The SDLC policy will make sure that security is integrated into every phase of system/software development. The policy puts an emphasis on secure coding practices, vulnerability assessments, and the use of encryption.

System or Software Patch Management Policy

This policy outlines the process for identifying, testing, and deploying security patches to systems and software. Patches are categorized by criticality and must be applied within specific timeframes to remove security vulnerabilities.

Security Maturity Policy

The security maturity policy is used to make sure there are continuous improvements in SnowBe Online's security posture. This is done through annual assessments and quarterly reviews. The organization measures its maturity level and implements a Security Improvement Plan to address gaps.

Section 6: Exceptions/Exemptions

Exceptions to the policies outlined in this document may be granted under specific conditions. To request an exception, a formal request must be submitted to the CISO via the IT Service Desk, detailing the rationale and proposed mitigation measures. All exceptions are subject to periodic review to ensure they remain necessary and do not compromise the overall security posture.

Section 7: Version History Table

Version	Date	Description
1.0	2024-09-29	Initial Draft

Citations

- https://www.compliancewire.com/EduFlexCourses/Courses/C_769_4247/Assets/lang_1/jobaids/sample_security_plan.pdf
- https://www.ferc.gov/sites/default/files/2020-04/security-plan-example.pdf
- https://www.cisa.gov/sites/default/files/2023-10/CISA_AASB_Security_Planning_Workbook_508_Compliant_20230929.pdf
- https://gisf.ngo/wp-content/uploads/2020/02/2128-InterAction-2016-Security-Plan-Example.pdf
- https://www.gisf.ngo/wp-content/uploads/2021/11/Creating-effective-security-plans.pdf
- https://www.selectagents.gov/compliance/guidance/security-plan/docs/Security_Plan_Guidance.pdf
- https://natural-resources.canada.ca/sites/www.nrcan.gc.ca/files/mineralsmetals/pdf/mms-smm/expl-expl/pdf/20140522-G05-04E.pdf