SnowBe Online Security Policy Portfolio

Secure SDLC, Patch Management, Security Maturity & Threat Modeling

A three-policy security governance package for SnowBe Online, followed by analysis showing how threat modeling informs lifecycle security, maturity improvement, and the broader security plan.

PCI DSS | Security Policy | Secure SDLC | Patch Management | Threat Modeling | Security Maturity | Governance

AT A GLANCE

Scenario	SnowBe Online: fast-growing retailer preparing to go public, with AWS-hosted sales, a WordPress shopping cart, stored payment data and informal security practices
Deliverables	Three CISO-owned policies: System Development Life Cycle Security, System & Software Patch Management, Security Maturity Management
Analysis	How threat modeling fits the system life cycle, the software life cycle, security maturity, and the security plan and policies
Outcome	Policies tied to real risks, with defined owners, exceptions, compliance consequences and annual review

Sean Richard

sean@autom8ionlab.com · linkedin.com/in/a8l-sean-richard · +1.352.818.9694

Portfolio edition based on original Full Sail University coursework. Substantive project content is preserved; classroom-only submission headers were removed.

POLICY 01

System Development Life Cycle Security Policy

Policy owner	Chief Information Security Officer
Effective date	May 3, 2026
Review frequency	Annual or after major system changes
Applies to	Employees, contractors, consultants, vendors, developers, system administrators, and third parties involved in SnowBe Online systems or software.

Purpose

The purpose of this policy is to establish secure system development life cycle requirements for SnowBe Online. SnowBe processes online sales through an AWS-hosted website, stores customer information and purchase history, accepts credit card payments, operates storefronts in the United States and Europe, and uses on-premise and cloud-based servers. Because these systems support critical business operations and store sensitive customer and payment information, security must be included throughout the full system development life cycle.

Scope

This policy applies to all SnowBe systems, applications, databases, servers, cloud services, websites, payment systems, customer service systems, accounting systems, vendor applications, mobile devices, desktops, laptops, and supporting infrastructure. This policy also applies to all new systems, major updates, system replacements, integrations, and system retirements.

Policy statement

SnowBe Online shall incorporate security into every phase of the system development life cycle, including analysis, planning, design, development, testing, deployment, maintenance, evaluation, and disposal. Security shall not be treated as an afterthought or only as a final review before implementation. Security requirements, threat modeling, access control, data protection, audit logging, patching, secure configuration, and compliance requirements must be considered throughout the life cycle.

Policy requirements

Analysis

SnowBe shall identify business needs, system objectives, sensitive data, legal requirements, security risks, and compliance requirements. Systems that process customer information, purchase history, payment data, or employee records must be classified as sensitive.

Planning

Each system project shall include security requirements, required approvals, responsible owners, budget considerations, risk management needs, and compliance obligations. PCI-related systems must include PCI compliance requirements during planning.

Design	SnowBe shall conduct threat modeling for new systems, major updates, cloud architecture changes, payment processing changes, and systems that store or transmit sensitive information. The threat model shall identify assets, data flows, trust boundaries, actors, threats, vulnerabilities, and required mitigations.
Development	Secure coding practices must be followed. Developers and technical staff must avoid hardcoded credentials, insecure protocols, weak authentication, excessive permissions, poor input validation, and unsafe handling of customer data.
Testing	Security testing shall include vulnerability scanning, access control review, authentication testing, patch verification, audit log validation, and testing of sensitive data protections. Systems that fail security testing may not be approved for production until issues are remediated or formally risk accepted.
Deployment	Systems must be securely configured before production use. This includes proper firewall rules, access control settings, logging, encryption, backup configuration, anti-virus protection, and approved patch levels.
Maintenance	Systems must be monitored, patched, backed up, reviewed, and updated. Login audit records must be retained for at least three months and archived to approved cloud storage after that period.
Evaluation	SnowBe shall review whether systems continue to meet business, security, compliance, and performance expectations. This review shall include technical controls, user access, patch status, backup status, audit logs, and threat model updates.
Disposal	Retired systems, devices, media, data stores, and cloud resources must be securely decommissioned. Customer data, payment data, and company records must be retained or destroyed according to legal, business, and compliance requirements.

Roles and responsibilities

The CISO is responsible for maintaining this policy and ensuring security requirements are included in the system development life cycle. IT and cybersecurity staff are responsible for implementing controls, performing reviews, maintaining documentation, and reporting risks. System owners are responsible for ensuring systems meet business and security requirements. Developers, vendors, and contractors are responsible for following secure development and configuration requirements. Management is responsible for ensuring projects receive adequate resources and oversight.

Compliance

Failure to follow this policy may result in increased business risk, disciplinary action, contract review, system deployment delays, or removal of system access. Exceptions must be approved by the CISO and documented with a business justification, risk rating, compensating controls, and expiration date.

POLICY 02

System and Software Patch Management Policy

Policy owner	Chief Information Security Officer
Effective date	May 3, 2026
Review frequency	Annual or after major security incidents
Applies to	Employees, contractors, consultants, vendors, system administrators, IT staff, developers, and any users responsible for SnowBe systems or software.

Purpose

The purpose of this policy is to establish patch management requirements for SnowBe Online systems, software, firmware, endpoints, servers, cloud services, and business applications. SnowBe uses desktops, laptops, on-premise servers, AWS-hosted systems, network devices, anti-virus software, backup software, VPN access, WordPress shopping cart functionality, and payment-related systems. These assets must be updated and maintained to reduce vulnerabilities and protect business operations.

Scope

This policy applies to all SnowBe-owned or SnowBe-managed hardware, software, operating systems, applications, firmware, network devices, mobile devices, cloud systems, storefront systems, servers, laptops, desktops, VPN services, anti-virus software, backup software, and WordPress components. It also applies to third-party systems that connect to SnowBe data or services.

Policy statement

SnowBe Online shall maintain a formal patch management process to identify, prioritize, test, approve, deploy, verify, and document patches. Patch management shall include operating system updates, server updates, endpoint updates, firmware updates, WordPress updates, shopping cart updates, anti-virus updates, backup software updates, and security updates for business applications. Patching shall be based on risk, criticality, system exposure, and business impact.

Policy requirements

SnowBe shall maintain an accurate inventory of all systems and software that require patching. This inventory shall include desktops, laptops, servers, network devices, AWS systems, WordPress components, VPN services, anti-virus tools, backup tools, and business applications.

Critical patches addressing actively exploited vulnerabilities, internet-facing systems, payment systems, remote access systems, or customer data systems must be prioritized for rapid review and deployment. High-risk patches must be reviewed and deployed within an approved timeframe based on severity and business impact. Medium and low-risk patches shall be deployed during scheduled maintenance windows.

All network device firmware must be reviewed and updated as needed. This includes firewalls, routers, switches, wireless access points, and VPN-related devices. All PCs and Windows servers must be updated to approved supported versions and maintained with current security patches. Anti-virus and backup software must be updated regularly to ensure protection and recovery capabilities remain effective.

SnowBe's WordPress shopping cart must be patched and reviewed regularly because it supports online transactions and customer purchasing. Payment-related systems must meet PCI compliance requirements.

Patches must be tested before deployment when practical, especially for critical systems such as order management, accounting, customer relations management, access management, storage, and vendor applications. Testing should confirm that patches do not disrupt normal business functions.

Patches must be approved before deployment. Emergency patches may be deployed faster when the risk of delay is greater than the risk of implementation. Emergency patching decisions must be documented.

Patch deployment must include verification. IT staff must confirm whether patches were successfully installed, failed, or require additional remediation. Failed patches must be tracked until resolved.

Mobile devices must be reviewed and approved before accessing company data. Devices that do not meet patch and security requirements may not access SnowBe systems.

Roles and responsibilities

The CISO is responsible for patch management oversight and policy approval. IT staff are responsible for identifying, testing, deploying, verifying, and documenting patches. System owners are responsible for coordinating maintenance windows and validating business functionality after patching. Employees and contractors are responsible for allowing updates to install and reporting system issues. Vendors must follow SnowBe patch management requirements when managing systems connected to SnowBe data.

Compliance

Systems that are unsupported, unpatched, or unable to meet minimum security requirements may be removed from the network or restricted from accessing company data. Exceptions must be documented, approved by the CISO, and include compensating controls and an expiration date.

POLICY 03

Security Maturity Management Policy

Policy owner	Chief Information Security Officer
Effective date	May 3, 2026
Review frequency	Annual or after major organizational or technical changes
Applies to	Executive leadership, IT, cybersecurity, system owners, process owners, employees, contractors, and vendors supporting SnowBe systems.

Purpose

The purpose of this policy is to establish a structured approach for measuring and improving SnowBe Online's cybersecurity maturity. SnowBe grew quickly and reached a high level of sales while operating with a laid-back culture and limited technical controls. Because the company is preparing to go public and stores sensitive customer, payment, and business information, SnowBe must move from informal security practices to structured, repeatable, measurable, and continuously improving security processes.

Scope

This policy applies to all SnowBe cybersecurity domains, including access control, asset management, audit logging, awareness and training, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, recovery, risk management, security assessment, situational awareness, system and communications protection, and system and information integrity.

Policy statement

SnowBe Online shall measure cybersecurity maturity at least annually and after major changes to systems, business operations, compliance obligations, or threat conditions. Security maturity shall be used to identify weaknesses, prioritize improvements, assign ownership, track remediation, and improve the overall security posture of the company.

Policy requirements

SnowBe shall maintain a security maturity assessment process that evaluates the organization's cybersecurity practices and processes. The assessment shall review whether security controls are ad hoc, documented, repeatable, managed, or optimized.

Security maturity assessments must include technical, administrative, and physical controls. This includes reviewing access management, patching, audit logging, incident response, backup and recovery, mobile device approval, physical server protection, PCI compliance, WordPress shopping cart security, anti-virus protection, risk management, and cloud storage practices.

The CISO shall establish maturity targets for each major security domain. Domains involving customer information, credit card data, AWS systems, remote access, audit logging, and access management shall receive higher priority because they directly affect business risk.

SnowBe shall document all maturity gaps and assign owners for remediation. Each gap shall include a description, affected systems, risk level, required improvement, responsible owner, target completion date, and status.

Security maturity improvement shall be tied to threat modeling, risk management, and security planning. When threat modeling identifies design weaknesses or control gaps, those findings must be reviewed as part of SnowBe's maturity improvement process.

SnowBe shall report maturity progress to management at least annually. Reports should include current maturity level, high-risk gaps, completed improvements, overdue remediation items, and recommended next steps.

Roles and responsibilities

The CISO is responsible for managing the security maturity program and reporting results to leadership. IT and cybersecurity staff are responsible for supporting assessments, implementing improvements, and documenting evidence. System owners are responsible for remediating assigned gaps. Executive leadership is responsible for supporting security maturity goals and providing resources when required.

Compliance

Failure to participate in maturity assessments or remediate assigned security gaps may result in escalation to management. Exceptions must be approved by the CISO and include business justification, risk acceptance, compensating controls, and a review date.

SECURITY PLAN UPDATES

Three new policies, summarized for the security plan

01 System Development Life Cycle Security Policy

Establishes security requirements for all SnowBe systems throughout analysis, planning, design, development, testing, deployment, maintenance, evaluation, and disposal. This policy ensures that security is built into the full life cycle instead of being added after systems are already deployed. It requires threat modeling, secure design, secure development, security testing, access control review, audit logging, patch consideration, data protection, and secure disposal. This policy is especially important for SnowBe because the company processes online sales, stores customer and payment information, uses AWS-hosted systems, and operates multiple business applications across cloud and on-premise environments.

02 System and Software Patch Management Policy

Defines how SnowBe identifies, prioritizes, tests, approves, deploys, verifies, and documents patches across company systems. This policy applies to desktops, laptops, servers, AWS systems, network devices, firmware, anti-virus software, backup software, WordPress components, VPN services, and business applications. The policy helps reduce the likelihood of exploitation by ensuring vulnerable systems are updated in a timely and controlled manner. It also supports PCI compliance, endpoint security, system reliability, and business continuity.

03 Security Maturity Management Policy

Establishes a formal process for measuring and improving SnowBe's cybersecurity maturity. This policy requires annual maturity assessments, domain-level maturity ratings, gap documentation, assigned remediation ownership, progress tracking, and management reporting. It helps SnowBe move away from informal security practices and toward repeatable, measurable, and continuously improving security processes. This policy supports SnowBe's growth, public company readiness, risk management goals, and need to protect customer information, credit card data, internal systems, and cloud-hosted business operations.

ANALYSIS

Where threat modeling fits

In the system development life cycle

Threat modeling fits into the system development life cycle because it helps identify security concerns before they become expensive or difficult to fix. In SnowBe's case, the company has many interconnected systems, including AWS-hosted website services, on-premise servers, customer databases, order management, accounting systems, laptops using VPN access, and storefront payment systems. Threat modeling helps the company understand how these systems interact, where sensitive information flows, and where trust boundaries exist. During analysis and planning, threat modeling helps identify important assets such as customer information, credit card data, login records, and business applications. During design, it helps identify weaknesses such as excessive access, insecure data storage, missing logging, weak network segmentation, or unpatched systems. During development and testing, threat modeling supports security requirements and test cases. During deployment and maintenance, it helps ensure controls remain effective as systems change. During evaluation and disposal, it helps confirm that risks are reviewed and sensitive data is properly protected or removed. Overall, threat modeling strengthens the SDLC by making security intentional across every phase.

In the software development life cycle

Threat modeling fits into the software development life cycle by helping developers identify how software can be misused, attacked, or designed insecurely. This is different from the broader system development life cycle because the focus is specifically on software, code, application logic, user input, authentication, authorization, data handling, and secure deployment. For SnowBe, the WordPress shopping cart is a major software concern because it supports online purchases and customer transactions. Threat modeling can help identify software risks such as insecure plugins, poor input validation, weak authentication, unpatched components, exposed payment data, excessive database permissions, session hijacking, SQL injection, cross-site scripting, and insecure handling of customer records. During software planning, threat modeling helps define secure requirements. During design, it helps developers understand data flows and possible attack paths. During coding, it supports secure coding practices and least privilege. During testing, it helps create security test cases based on actual threats. During deployment and maintenance, it supports patching, monitoring, and secure configuration. Threat modeling makes software development stronger because it forces the team to think about what could go wrong before attackers do.

In security maturity

Threat modeling fits into security maturity because it helps an organization move from reactive security to proactive and repeatable security practices. An immature organization may only respond after something breaks or after a vulnerability is exploited. A more mature organization identifies risks earlier, documents them, assigns ownership, and tracks remediation. SnowBe is a good example of a company that grew quickly but did not build strong security processes early. The company added technical controls later, such as patching, anti-virus, backups, access management, and audit logging, but security maturity requires more than tools. Threat modeling improves maturity by creating a structured method to identify assets, data flows, trust boundaries, threats, vulnerabilities, and mitigations. It also creates useful documentation that can be reviewed and updated as systems change. As SnowBe

performs threat modeling regularly, the company can improve repeatability, reduce design flaws, create better security requirements, strengthen testing, and support risk-based decision-making. Over time, this helps SnowBe move toward a more mature security program where security is measured, managed, and continuously improved rather than handled informally.

In the security plan and policies

Threat modeling fits into the security plan and policies because it provides evidence-based direction for what policies should require and what risks the security plan must address. A security plan should not be a generic document that lists controls without understanding the organization's actual systems. Threat modeling helps SnowBe identify where its sensitive data lives, how customer and payment information moves through systems, where trust boundaries exist, and which systems are most exposed. This information can improve policies for access control, patch management, audit logging, incident response, secure development, mobile device access, cloud storage, and data retention. For example, SnowBe's threat model may show that excessive employee access to server data creates a major risk. That finding should influence the access management policy. If the threat model shows that the WordPress shopping cart is exposed to internet-based threats, that should influence patch management and software security requirements. If threat modeling identifies missing logs, that should strengthen audit policy requirements. Threat modeling keeps the security plan practical because it connects policies to real risks, real systems, and real business needs.