External-Facing Information Security Framework

Global Security Office (GSO)

Version 2.8

Last Updated: 05/09/2017

Symantec Corporation

Table of Contents

Compliance Framework

Symantec is committed to the protection of the company's information technology, brand, intellectual property, personal information and customer data from misuse or compromise. This external-facing framework defines how Symantec protects its assets and reputation from threats associated with misuse or compromise of information/data. This includes whether the threat is internal or external, deliberate or accidental in nature.

All parties under the scope of this external-facing framework must abide by the following core principles:

Regulatory/Legal Compliance: The company shall achieve and maintain compliance with all applicable laws and regulations.

Follow Industry Recognized Guidance: Symantec uses the following industry guidance in the development and review of company security requirements and controls: International Organization for Standardization (ISO) 27001:2005 and ISO 27002:2005.

- Payment Card Industry (PCI) Data Security Standard (DSS)
- National Institute of Standards and Technology (NIST) Special Publications (SP) and Cyber Security Framework
- The Open Web Application Security Project (OWASP)

Protections based on information classification: Application of appropriate security controls is based on having managed information classified by category of information. Managed data and information is classified according to the potential risk and impact of exposure. Therefore, an information classification method will be utilized to determine the protection requirements for managed data. Managed data and information in higher risk classifications will have more stringent control requirements.

Be accountable: Roles and responsibilities for access to managed data are defined, communicated and acknowledged to establish and maintain accountability for security within the organization.

Integrate security within the business: Information security considerations are incorporated into all areas of the business so they are integrated into business processes and ongoing daily routines. This includes a continuous improvement approach to building in security controls within application or product development lifecycles.

Foster a security culture: Management will promote a security-minded culture by providing ongoing education and awareness of security topics. A company information security program is responsible for ensuring ongoing education, awareness and administration of activities related to policy compliance.

Manage security risk: Risks to information confidentiality, integrity or availability are actively managed. Threats and vulnerabilities must therefore be identified and risk potential must be assessed. Identified risks are documented, mitigated with internal controls, and reported to management in a timely manner.

Measure and report: Adherence to the information security framework and program components is actively monitored, measured, and reported.

Investigate and respond to incidents: Breaches of information security controls, actual or suspected, must be reported to management and the Global Security Office Incident Response Team in a timely manner. Each incident will be investigated thoroughly and credibly, consistent with industry best forensic and investigation practices. Responses to incidents will follow established guidelines.

Maintain continuous business operations: Business operations are regularly evaluated to establish a hierarchy of critical functions and/or systems. Business continuity management processes are established to provide a framework for building resilience into operations and the capability for an effective response in the event of an operational incident.

High-Level Information Security Program

The *Information Security Framework* establishes the information security principles at Symantec, but does not detail every security control or technical requirement. Detailed security requirements are documented in other classes of documentation in a hierarchy that becomes progressively more specific.

Symantec's Information Security Program consists of the following classes of documentation:

Information Security Framework: defines information security management and governance requirements within the company and provides the principles for the Information Security Program.

Security Standards: contain mandatory internal controls designed to provide the Information Security Framework with the support structure and specific directions it requires. Controls within the security standards are derived from the international security standard ISO 27001/27002. These may also be further detailed by requirements from the PCI DSS or NIST special publications as applicable.

Security Methods: contain mandatory configuration settings derived from controls established in the security standards. These documents define configuration settings for a specific technology platform or application.

Security Guidelines: provide advisory information and guidance to assist in the implementation of security controls. Guidelines do not establish controls and therefore contain no mandatory requirements. They serve as additional support in implementing the defined standards.

Compliance

All employees, contractors, consultants, service providers, partners, or entities acting on behalf of Symantec must adhere to this *Information Security Framework*. This is inclusive of all supporting standards in the Information Security Program.

Before accessing or using Symantec resources, employees must review and agree to adhere to the *Information Security Framework*.

Violations

Any Symantec employee that violates the *Information Security Framework* may be subject to disciplinary action up to and including termination of employment. Additionally, any individual who violates this framework may be subject to civil penalties or criminal prosecution under applicable laws or government regulations. In addition to reporting incidents to management and Global Security Intelligence Operations (GSIO), framework violations or related misconduct should be reported to Symantec's Ethics Line. Where permitted, a report can be made anonymously. Retaliation against anyone who makes such a report in good faith is prohibited.

Information systems will be regularly checked for compliance with security policies and standards. All areas within the company are subject to regular reviews to ensure compliance with security policies and standards.

Audit of Third-Party Service Providers

Where applicable, third parties must be engaged through the Vendor Management Program. Symantec non-public data may only be shared with third parties upon signing of a Non-Disclosure Agreement. GSO has the responsibility for audits of our third party capabilities to ensure compliance with all applicable Symantec information security policies.

Where applicable, third-party service provisions in all master services or consulting agreements for outsourced services include a right to audit clause, allowing Symantec to audit that entity at will. Additionally, contracts require outsourced entities to provide Symantec a copy of its third-party security audit documentation (i.e., ISO 27001 certificate with corresponding Statement of Applicability or SOC 2 Type II report), where appropriate. The risks associated with access to the company's information systems by third parties must be continually assessed and appropriate security controls must be implemented.

Ownership and Authority

Title	External-Facing Information Security Framework
Organization/Authority	Global Security Office
Last Review Date	04/06/2017
Impacted Functions/Audience	DL-IT-Information Security Team
For questions about this standard, contact:	DL-GSO-Security-Policy@symantec.com

Document History

Approval

Approver	Version	Date
SGRC	2.6	03/23/2015
SGRC	2.7	02/23/2016
Governance & Risk Management (GRM)	2.8	04/06/2017

Revision

Change Reference	Version	Date
Revision 2.0 draft	2.0	03/21/2013
Incorporated comments from internal SGRC review to draft v2.	2.1	04/05/2013
Incorporated comments from working group (Legal, ITS, HR, GSO safety & security) to draft v2.2	2.2	04/18/2013
Incorporated comments from working group, extended reviewers (from Legal), and GSO management into draft v2.3	2.3	05/13/2013
Revised for new nomenclature.	2.4	01/17/2014
Revised to be Customer Facing	2.5	07/22/2014
Reviewed information, updated content to reflect organizational changes, moved content to the new policy template, reviewed for minor grammar and style issues, and published.	2.6	03/23/2015
Revised to be External Facing; also updated the “Audit of Third-Party Service Providers” section to include third-party security audit documentation.	2.7	2/23/2016
Various updates throughout the document, including adding the Cyber Security Framework to the recognized guidance section under “Compliance Framework”.	2.8	4/6/2017