Global Security Office

At Symantec, we are dedicated to each other, our customers, our business, and society. We believe that information protection is a central element of our responsibility. The very nature of our business requires a culture of security responsibility.

Symantec's **Global Security Office (GSO)** is responsible for maturing Symantec's Information Security posture by supporting our global culture of security and protecting information assets and technologies to secure your information whereve it lives. The GSO is comprised of dedicated team based all around the world who work together to provide visibility and continuously enhance the security over Symantec's applications and networks.

The **Governance, Risk & Compliance (GRC) team** strives to achieve the highest level of cyber security by establishing policy, governing risk, and managing compliance. Our goal is to safeguard Symantec's technology, brand, intellectual property, and customer data from misuse or compromise while driving the effectiveness of the information security program.

The **Security Assurance (SA) team** provides compliance and assurance services to Symantec customers, lines of business and suppliers - to maintain and improve the high security standards we expect, and are expected of us. The team operates a global capability operating across all regions, serving Symantec customers wherever they do business. The Supplier Assurance function manages the Third Party Risk Management program in categorising and evaluating suppliers to ensure their security practices align with Symantec standards. The Product Assurance function perform an internal audit role in evaluating our products against industry-standard baselines and frameworks.

Symantec's **Trust and Safety team** aim to cultivate a more resilient organization by empowering staff with the tools and knowledge they need to help protect Symantec. We promote a security-conscious culture under which staff internalize security policies and procedures and habitually put them into practice, and commonplace security weaknesses are normalized and managed effectively. Our programs help staff work with greater confidence and drive a measurable impact on reducing information security risks caused by human error or negligence. Our activities include security awareness training, application security training, vulnerability reporting programs and outreach.

The **Security Architecture and Engineering (SAE) team** works together to ensure security is built into Symantec's development and operations. The architecture team performs reviews over application and network designs, while the software security team ensures appropriate reviews are performed at all stages of the software systems development lifecycle.

The **Physical Security and Safety team** is committed to protecting our employees, assets, facilities and brand reputation from compromise, loss or destruction. They ensure our employees and guests are provided the safest, most secure environment within which to operate. They have the tools and resources to effectively manage proactive and rapid reactive security responses at facilities worldwide.

The **Enterprise Resilience team** manages operational and technology risk that could impact Symantec's ability to deliver services to customers. Our Business Continuity and Disaster Recovery program focuses on identifying actual and potential risks to business functions, partnering with the business to mitigate those risks. The **Crisis Management program** provides a framework, centralized command and control to coordinate, facilitate and support consistent, effective responses when there is an interruption to business, safeguarding the interests of employees, customers, partners and shareholders.

The **Defensive Cyber Operations (DCO) team** provides continuous monitoring of all Symantec information systems and assets to identify cyber security events and verify the effectiveness of all protective measures deployed. They are focused on the detection of anomalous activities and understanding the potential impacts in a timely manner. Our vulnerability management program is designed to proactively prevent the exploitation of vulnerabilities and reduce threats to Symantec's infrastructure. To promote security situational awareness, our Threat Intelligence team provides a framework of Indicator of Compromises (IOCs) from a collection of proprietary threat intelligence feeds. These are critical to maintaining the operational availability, confidentiality and integrity of information technology systems used internally by Symantec employees and to support customers.

The **Offensive Security team** protects Symantec and its customers by applying adversarial methods to improve our security posture and resilience to current and emerging threats. To ensure adequate security controls and processes are in place, they conduct general penetration tests against all of Symantec's assets and infrastructure. This may involve penetration testing, external network, internal network, wireless network, etc. The Offensive Security tram continually challenges the status quo, innovating new wats to emulate malicious adversaries and their tactics, techniques and procedures. This understanding of how attacks operate improves out detection capabilities and effectiveness of our security posture.

The **Protective Cyber Services team** is focused on ensuring Symantec's cyber security controls and related processes are operating at their fullest capacity providing consistent outcomes that enable the business. The team secures the company today, reducing risk by effectively running the technologies and continuously measuring key security metrics. The service portfolio includes endpoint protection, network protection, data protection, threat/vulnerability management and crypto domains.