

Job Purpose

The Information Security Manager is responsible for the operational security of Endace's IT infrastructure and for setting standards and procedures to ensure Information Security concepts are embedded in all systems, including the network, operating systems and applications.

This position is responsible for vulnerability scanning and remediation, proactive security measures designed to manage and minimise risk to the organisation, as well as leading security incident response activities. They act as an Information Security leadership figure in the company, and are responsible for championing security across the organisation.

Key Responsibilities

Technical

- Maintain the Endace Information Security Management System (ISMS)
- Define, document and maintain processes and best practices to ensure security concepts are embedded in day-to-day operational and development procedures
- Develop, maintain and operate comprehensive vulnerability scanning and security testing frameworks and toolsets to proactively identify security issues on the network, server and desktop operating systems, and applications
- Establish and maintain tools and processes to perform monitoring, intrusion detection and alerting of malicious activity across networks to enable incidents to be detected
- Responsible for Security Incident Response
- Ensure proactive and secure management of passwords, SSL certificates and other encryption keys
- Develop and maintain appropriate tools and processes to ensure that Endace can meet its legislative and commercial obligations as they relate to Information Security
- Act as the privacy officer for Endace.
- Champion good Information Security practices across the company, and represent Endace in the wider IT security community
- Work with the IT Manager to support compliance assessment and reporting, and the management of the IT Risk Register and IT Asset Register
- Work with the IT Manager to consult in the development of IT policy, including identity and access management and device security
- Work closely and effectively with other members of the IT team to ensure best practice Information Security is adopted and put in place and roadmaps are aligned. Share resources for project implementation
- Ensure that security controls are well defined, appropriate and workable
- Work within a cross functional team to ensure that physical security needs are implemented globally
- Develop and maintain contact and relationships with internal teams and stakeholders to understand their security, technology, support, and infrastructure needs
- Work with various FUSION partners to trial their analytics in our system, providing feedback to marketing and FUSION teams
- Work with Legal and Procurement teams to make sure security standards are embedded in our supply chain, and to answer customer requirements
- Contribute to the development and maintenance of a security road map of projects and improvements
- Prepare security budgets and keep track of expenditure against budgets
- Lead Information Security projects as required.

Organisation

- Complete and ensure others complete administrative tasks in an accurate and timely manner
- Champion safe working practice of self and others in accordance with Health and Safety Procedures
- Observe, comply and provide significant input into developing policies, procedures and strategy and quality management systems
- Model effective communication and champion the provision of constructive feedback
- Support and positively champion Endace’s overall organisational vision, values and culture
- Be a source of specialist advice on approaches, products, services, market conditions and opportunities
- Complete, participate in and ensure other’s undertake Career Development Planning.

Competency Profile

Technical

- A degree in Computer Science or equivalent demonstrable business experience
- Must have a minimum of 5 years’ experience in Information Security
- Practical experience in incident response, securing networks, applications and operating systems is essential
- Proven ability to provide thought leadership to a technical team
- Excellent written and verbal communication skills are required with the ability to present to an audience.
- Experience managing multiple technology suppliers to deliver an integrated roadmap
- Ability to document and maintain policies and procedures
- Solid knowledge of endpoint security, protection strategies, and forensic examination
- A thorough understanding of network protocols and cloud security
- Ability to occasionally work outside of standard office working hours
- Ability to travel, internationally and domestically, as required.

Core

Interpersonal Skills

Understands the attitudes, interests, needs and perspectives of others. Able to interpret non-verbal behaviour of others such as moods and feelings, with the capability of adapting behaviour to different situations.

Listens carefully and non-defensively to various points of view whether or not they agree with these.

Achievement Drive and Energy

Strong drive for success and relentless pursuit of achieving results.

Dedicated, committed, enthusiastic, positive, and motivated. Has courage and persistence in convictions no matter how difficult the task.

Is action oriented and pursues everything with energy and drive.

Planning, Organizing and Prioritizing

Passionate about success and winning.

Devises and drives work plans that have localised impact.

Keeps a view of business priorities and redefines own and team’s priorities in line with expectations and objectives.

Communication Skills

Able to communicate logically, clearly, effectively, and confidently at all levels.

Listens intently and ensures other party feels they have been heard and understood.

Can convince across functional areas, completing and often opposing views to gain agreement.

Tolerance to Ambiguity

Is consistently drawing together and presenting reasonable conclusions from incomplete evidence and data.

Takes action and provides clarity for other in situations where details are not clear.

Customer

Promotes an attitude of valuing customers.

Advocates for the inclusion of customer interests and needs in programme planning and decision making.

Empowering Others

Guides and develops others to generate performance consistent with organizational goals and values.

Enables people to act and holds them accountable for their actions.

Change Orientation

Develops change strategies at department level and provides leadership through change.

Facilitates change and ownership in own areas and across business units and stakeholders.

Competitive Edge

- An understanding of software development processes and common programming vulnerabilities
- Experience working within security communities (e.g. CERT, NZITF, REN-ISAC, First.org or others).

Date: November 2022
Title: Information Security Manager
Position Reference: END110
Department: Operations, IT
Physical Location: Auckland or Hamilton
Responsible to: Vice President Operations

Job Code: 33070
Level: Corporate 5
Employment Status: Permanent
Hours: Fulltime
Budget Level: As per delegated authorities policy
Team Leadership: None