Everest engineering

Roles and responsibilities

ISM.02

Version 0.2.3

July 1 2025

Contents

1 Introduction

This document defines the security roles and responsibilities for implementation and continual improvement of Everest Engineering's security posture.

2 Roles

2.1 ISMS Council

The ISMS council comprises the executive management (CEO and CTO) and delegated representative roles.

The members are:

- CEO;
- CTO;
- director of information security;
- the information security team; and
- function directors.

2.2 Director of information security

The director of information security is responsible for advocating and driving information security practices at functional levels within Everest Engineering. They are responsible for coordinating ISMS activities throughout the organisation.

2.3 Function directors

This group owns identified risks and has the authority to delegate treatment within their functions. Members are responsible for tracking and reporting progress towards compliance to the ISMS council.

Risk owners – those assigned responsibility to address risk – report their progress to their function director to assess, audit and review treatment effectiveness.

2.4 Information security team

This team is responsible for day-to-day security compliance and monitoring throughout the organisation to achieve the goals of the ISMS.

Individuals within this team have a deep technical understanding of information networks, software application security and general security practices.

2.5 Employees and contractors

This group comprises all individuals who are employed by Everest Engineering.

3 Responsibilities

3.1 ISMS council

Annual responsibilities:

- review of information security policy and establishment of security goals aligned with Everest Engineering's strategic direction;
- allocation of budget and resourcing to support the ISMS;

- communication of the importance of the ISMS and expectations around adhering to security requirements;
- review of security training and awareness training; and
- management of annual internal security audits.

Quarterly or as-needed responsibilities:

- review of metrics tracking both technical and process adherence to the ISMS.

Continuous responsibilities:

- promotion of continuous improvements;
- ISMS documentation management.

3.2 Function directors

Quarterly responsibilities:

- review of organisational processes to ensure ISMS requirements are met;
- review and assessment of risks tracked in the risk register;
- delegation and tracking of risk treatment; and
- reporting risks and treatment progress to the ISMS council.

Continuous responsibilities:

- supporting the implementation of the ISMS within their functions.

3.3 Information security team

Continuous and as-needed responsibilities:

- maintain the register of relevant authorities and the circumstances in which they may be contacted;
- maintaining professional relationships with relevant special interest groups in order to stay up to date with security developments and to gain access to a professional support network;
- support of change management and driving corrective actions throughout the organisation;
- incident management including post-incident reviews, and communication of trends and learnings;
- ISMS exemption tracking and monitoring;
- collection of metrics demonstrating technical and process effectiveness in ISMS compliance; and
- performing internal audits, assisting with external audits and management reviews.

3.4 Employees and contractors

Continuous and as-needed responsibilities:

- active participation in security training and security awareness;
- protection of information and device assets, including data security classification and labelling, protection of removal media, and proper disposal of information assets; and
- understanding and compliance with ISMS security policy, including: mobile device, anti-malware, electronic messaging, acceptable use, personal information protection, and social media policies.