Everest engineering

Acceptable use policy

ISM.09

Version 0.2.3

July 1 2025

Contents

1 Introduction

This policy covers of use of information assets and information processing facilities by Everest Engineering staff. Its goal is to protect individuals, the company, our customers, and third parties.

1.1 Scope

This policy applies to all Everest Engineering permanent employees, contractors, advisors and contracted partners using, or granted access to, information assets and information processing facilities owned by Everest Engineering, our customers (whether contracted or not) and third party partners.

2 Acceptable Use

2.1 Data security classification

All information assets, whether in digital or physical form, that are owned by Everest Engineering or one of our customers must be handled according to our data security classification scheme.

2.1.1 Classified information

Confidential and highly confidential information must be encrypted prior to transmission over insecure channels such as email.

Classified information assets must be destroyed when they are no longer required to be stored on local devices. Classified information assets may only be stored and accessed on devices that:

- are classified with a same or higher level (more restrictive) security classification; and
- are secured with Everest Engineering approved endpoint protection.

2.1.2 Public information

Copyrights, licenses, trade secrets and patents must be respected.

2.2 User credentials

Your Everest Engineering single-sign-on (SSO) and local account credentials may not be shared with any other person. Passwords must meet the requirements of our password complexity policy and may not be stored in cleartext in digital or physical form.

The use of approved password managers is highly recommended.

2.3 Physical security

Classified information must only be accessed when working in an environment where it is not visible to unauthorised individuals.

Devices must not be left unattended in public spaces or in private spaces easily accessible to the public. This includes being left unattended in a car or in the boot of a car.

Equipment may not be removed from Everest Engineering facilities without approval.

2.4 Access controls

Controls limiting access to networks, systems or applications must not be circumvented. Unauthorised access to systems is not permitted.

2.5 Social media

Any use of social media must comply with our social media policy.

2.6 Return of assets

All Everest Engineering owned devices must be returned on separation from the company.

2.7 Compliance

Everest Engineering will verify policy compliance through various methods. This includes audits, automated reporting, and feedback to information asset owners.

Intentional violation of policy may be subject to disciplinary action, including termination of employment.