Everest engineering

Physical security policy

ISM.05

Version 0.2.3

July 1 2025

Contents

1 Introduction

This policy describes the physical security controls required to protect our employees, contractors and assets.

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 Secure areas

Secure areas are buildings, rooms or otherwise physically segregated areas whose purpose is to securely store information assets or information processing facilities. These are distinct from insecure areas such as collaborative working spaces where mobile devices are removed at the end of the day.

Selecting appropriate controls for a secure area requires risk assessment given the data classification of the assets being protected.

2.1 Building and perimeter controls

Physical security begins with the building itself and its perimeter. Appropriate control mechanisms may include:

- alarms fitted and activated outside working hours;
- window and door locks;
- window bars on lower floor levels;
- access control mechanisms fitted to all accessible doors (where codes are utilised, they should be regularly changed and known only to those people authorised to access the area);
- auditable access logs which are to be retained for at least 60 days;
- video surveillance around building exteriors and build ingress areas;
- staffed reception areas; and
- protections against fire, flood, and vandalism.

2.2 Personnel access

Staff working in secure areas must challenge anyone who does not appear to belong in the area.

Identification, and access tools and passes such as badges, keys, and entry codes must only be held by individuals authorised to access those areas. They must not be shared or given to others.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge.

All visitors accessing a secure area must be monitored by an employee authorised to access the area.

Where breaches do occur, or an employee leaves outside normal termination circumstances, all identification and access tools and passes must be recovered from the employee and any access codes should be changed immediately.

2.3 Paper and equipment security

Everest Engineering's data classification scheme also applies to physical information assets such as paper copies. These must be protected by building controls and via appropriate measures that include:

- filing cabinets that are locked with the keys stored away from the cabinet;
- locked safes; and
- stored in a secure area protected by access controls.

All general computer equipment must be in suitable physical locations that:

- limits the risks from environmental hazards such as heat, fire, smoke, water, dust and vibration;
- limit the risk of theft such as physically attaching machines to desks or securing them in an equipment rack; and
- allows workstations handling sensitive information to be positioned to eliminate the risk of the data being seen by unauthorised people.

Business critical systems should be protected by an uninterruptible power supply depending on their criticality.

Cables that carry data or support key information services must be protected from interception or damage. Network cables must be protected by conduit and where possible avoid routes through public areas.

3 Equipment lifecycle management

Staff involved with asset maintenance must, where appropriate:

- retain all copies of manufacturer's instructions;
- identify recommended service intervals and specifications;
- enable a call-out process in event of failure;
- ensure only authorised technicians complete any work on the equipment;
- record details of all work carried out;
- identify any insurance requirements; and
- record details of faults incurred, and actions required in the asset register.

A service history record of equipment must be maintained so that decisions can be made regarding the appropriate time for it to be replaced.

Manufacturer's maintenance instructions must be documented and available for support staff to use when arranging repairs.

The use of equipment off-site must be formally approved by the user's line manager.

Equipment that is to be reused or disposed of must be properly erased or destroyed. This includes returning equipment to a leasing provider.

Equipment deliveries must be signed for by an authorised individual and assets entered into the asset register as soon as is practical. Individuals receiving deliveries must verify that all items listed on delivery notes were received.