Everest engineering

Network security policy

ISM.07

Version 0.2.3

July 1 2025

Contents

1 Introduction

This policy describes Everest Engineering's rules, framework and standards for network protection. Its intended audience is Everest Engineering's IT service desk, information security, and developers designing and implementing both internal networks and those of our customers.

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 Network security design

Each network design will be unique in order to meet a set of specific requirements for an application, business function or customer project. This policy provides guidance for the standard building blocks that should be used to ensure that networks are designed to an appropriate degree of security.

Network requirements and the corresponding design for all Everest Engineering owned networks must be documented and approved by Everest Engineering's information security team before implementation work commences.

2.1 Requirements

A network design must be based on clear requirements which should include the following security-related factors:

- the classification of the information to be carried across the network and accessed through it;
- a risk assessment of the potential threats to the network, considering any inherent vulnerabilities;
- the level of trust between the different components or organisations that will be connected;
- the hours of availability and degree of resilience required from the network;
- the geographical spread of the network;
- the security controls in place at locations from which the network will be accessed; and
- security capabilities of existing computers or devices used for access.

2.2 Defence in depth

A defence in depth approach must be adopted to network security. Multiple layers of controls must be used to ensure that the failure of a single component does not compromise the network. For example, network firewalls may be supplemented by host-based software firewalls on servers and clients in order to provide several levels of firewall protection.

At key points in the network a defence diversity approach must also be taken so that vulnerabilities are minimised. For example, this may involve using firewalls from different vendors in series so that if a vulnerability is exploited in one device the other will not be subject to it. This may be extended to the use of more than one network virus scanner at the perimeter.

2.3 Network segregation

The principle must be adopted that, where appropriate, a network will consist of a set of smaller networks segregated from each other based on either trust levels or organisational boundaries (or both).

For a large network this may be achieved using separate domains, particularly where separate organisations' networks are being linked. An appropriate level of trust must be configured at the domain level and the domain perimeter must be secured using a firewall where appropriate.

Within networks, virtual local area networks (VLANs) must be used to segregate organisational units.

In a cloud environment, it is important that requirements for segregating networks to achieve tenant isolation are defined and the cloud service provider's ability to meet these requirements is verified.

Where Everest Engineering is acting as a software-as-a-service (SaaS) provider, it is important to enforce segregation between our multi-tenant clients and also between the cloud service customer environment and our own internal network.

2.4 Perimeter security

Measures must be in place to ensure that only authorised network traffic is permitted at the perimeters between internal and external networks. This will usually consist of at least one stateful inspection firewall and an application firewall or gateway at Internet links. For connections such as broadband at smaller locations a packet filtering firewall may suffice, depending on the results of a risk assessment.

Servers that are intended to be accessed from an external, insecure network must be located in a demilitarised zone (DMZ) of the firewall in order to provide additional protection for the internal network.

2.5 Public networks

Strong encryption must be used to ensure the confidentiality of data transmitted over public networks.

2.6 Wireless networks

Wireless networks must be secured using WPA2 or WPA3 encryption. WEP and WPA must not be used. Wireless networks must be treated as insecure even if WPA2 is used as the encryption method and a firewall installed between the wireless network and the main LAN.

A guest wireless network may be provided for visitors. This must be physically separate from all internal networks (including internal wireless networks) and secured using a firewall.

WiFi protected setup (WPS) must not be used. Wireless access point admin logon passwords must be changed from the default.

2.7 Physical security

Remote network equipment will be housed in secure cabinets that must be locked. Only authorised support staff may have access to the key to each cabinet.

Backbone and centralised network equipment will be housed in appropriate lockable cabinets or racks in a secure server room to which only authorised support staff will have access (except for local facilities staff for reasons of health and safety).

Wireless access points located in public areas must be hidden from view where possible and must be placed in positions where access by the public is difficult (such as in or near the ceiling). A lockable protective casing must be installed where an access point is in an unprotected public area such as a car park.

2.8 Remote access

Where there is a requirement for remote access to the internal network the following controls will be used:

- a virtual private network (VPN) will be used providing session encryption using SSL/TLS;
- two-factor authentication at the client where appropriate;
- secure authentication using a RADIUS server; and
- network access control (NAC) will be used to restrict access to remote clients that do not meet minimum requirements.

Remote access must be granted on an as-required basis rather than for all users by default.

2.9 Network intrusion detection

A network-based intrusion detection system (NIDS) must be installed at the network perimeter and at all key points within the network such as critical servers.

For networks with high security requirements an intrusion prevention system (IPS) may be considered, although its implementation should be approached with caution to avoid a high degree of false positives with corresponding disruption to service to users.

3 Network security standards

The following standards will be adopted with respect to network configuration and security.

3.1 Network hardware

Where possible a single supplier policy will be used for network hardware. An exception will be made where the use of multiple vendor hardware may increase the level of security provided.

Switch ports, including diagnostic ports, will be configured to be administratively disabled until required. Hubs will not be used due to their inherent security weaknesses.

Cat 6 UTP will be used for network cabling unless specific circumstances (such as excessive interference) preclude its use. The network topography used will be Ethernet according to the IEEE 802.3 family of standards.

3.2 IP addressing

IPv4 will be used on internal networks. However, new network devices purchased must support IPv6.

IP addresses and associated network information for desktop and laptop clients will be controlled using DHCP. Internal DNS servers will be used.

3.3 Network protocols

The protocol used on all networks will be TCP/IP. UDP will be used where appropriate but other OSI layer 4 network protocols should not be used.

Only protocols and ports required on a specific server will be enabled by default in order to reduce the attack surface.

4 Network security management

The following controls define how an existing network must be maintained in order to sustain information security.

4.1 Roles and responsibilities

Roles and responsibilities for the management and control of networks must be clearly defined. In order to provide effective segregation of duties, the operation of networks must be managed separately from the operation of the rest of the infrastructure such as servers and applications.

4.2 Logging and monitoring

Logging levels on network devices must be configured in accordance with Everest Engineering's policy and logs should be monitored on a regular basis.

Firewall logs will be monitored for signs of excessive port scanning which may be a precursor to a remote attack. Where installed, a network-based intrusion detection system must be configured to alert the network's operations team of this activity.

Network monitoring for availability may be achieved using an appropriate SNMP-based network management tool and recovery actions automated where possible.

Alerts from the network access control (NAC) system must be addressed immediately to ensure that clients that do not meet minimum security requirements are only allowed access to a quarantined subset of systems on the network.

4.3 Network changes

All changes to network devices will be subject to Everest Engineering's change management process and appropriate risk assessment, planning and back-out methods. Configuration records must be updated whenever such changes are carried out so that a current and accurate picture of the network is always maintained.

4.4 Network security incidents

Network events which are deemed to be security incidents must be recorded and managed following our incident management procedures.