E. Everest engineering

Access control policy

ISM.04

Version 0.2.3

July 1 2025

Contents

1 Introduction

This document describes our policy for selecting access controls and for granting individuals access to applications, services and systems.

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 Access control requirements

Access controls are required for all applications, services and systems. The level of control required depends on the needs of the business and must consider:

- the data security label assigned to the target application or system;
- local legislation and regulatory frameworks;
- contractual obligations; and
- risks identified through threat modeling.

An off-the-shelf application may not support the desired level of control. In this case, mitigating controls must be established based on the threat model.

All applications and systems developed for Everest Engineering and customer projects must have requirements for access control documented.

The following principles must be applied when designing access controls:

- **defence in depth**: security must not depend upon any single control but be the sum of several complementary controls;
- **least privilege**: the default approach taken must be to assume that access is not required rather than to assume that it is;
- **need to know**: access is only granted to the information required to perform a role;
- **need to use**: users will only be able to access physical and logical facilities required for their role; and
- **segregation of duties**: breaking tasks down into separate components along functional lines when risk for fraud or error exists.

3 User access management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure only authorised users have access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final removal of users who no longer require access.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

3.1 User registration and removal

A request for access to Everest Engineering's network and computer systems must be submitted to Everest Engineering's IT service desk. All requests must be handled using a standardised, auditable procedure to ensure that appropriate security checks are carried out and that correct authorisation is obtained prior to account creation.

Each user account must have a unique username that is assigned to an individual. It may not be shared with any other user. Generic user accounts (i.e., single accounts to be used by a group of people) must not be created as they provide insufficient allocation of responsibility.

An initial strong password must be created on account creation and communicated to the user via secure means. The user must be required to change the password on first use.

When an employee leaves the organisation under normal circumstances, their access to computer systems and data must be suspended at the close of business on their last working day unless a special exemption is approved by the information security team. It is the responsibility of the line manager to request the suspension of the access rights via Everest Engineering's IT service desk.

In exceptional circumstances where there is perceived to be a risk that the employee may take action that may harm the organisation prior to or upon termination, a request to remove access may be approved and actioned in advance of notice of termination being given. This precaution will especially apply in the case where the individual concerned has privileged access rights.

User accounts must be initially suspended or disabled only and not deleted. User account names must not be reused as this may cause confusion in the event of a later investigation.

3.2 User access provisioning

Each user must be allocated access rights and permissions to computer systems and data that are in line with the tasks they are expected to perform. In general, this will be role-based, *i.e.* a user account will be added to a group that has been created with the access permissions required by that job role.

Group roles must be maintained in line with business requirements and any changes to them must be formally authorised and controlled via the change management process.

Ad-hoc additional permissions must not be granted to user accounts outside the group role. If such permissions are required this must be addressed as a change and formally requested.

3.3 Removal or adjustment of access rights

Where an adjustment of access rights or permissions is required (such as an individual changing role) then this must be carried out as part of the role change. It must be ensured that access rights no longer required as part of the new role are removed from the user account. Consideration of any issues of segregation of duties must be given.

3.4 Management of privileged access rights

Privileged access rights such as those associated with administrator-level accounts must be identified for each system or network to be tightly controlled. When access control cannot be set up at the system level, a separate user account can be allocated to IT support desk staff (or other authorised Everest Engineering personnel) when additional privileges are required for handling administrative tasks for a specific system. Both types of account must be specific to the individual account holder, such as “John Smith Admin”, to provide sufficient identification of the user. Generic accounts such as “Corporate Admin” must not be used for assigning any type of account.

Access to admin level permissions must only be allocated to individuals whose roles require them and who have undertaken sufficient training for understanding the implications of administrative rights and their uses.

The use of user accounts with privileged access in automated routines such as batch or interface jobs must be avoided where possible. Where this is unavoidable the password used must be protected and changed on a regular basis.

3.5 User authentication for external connections

In line with our network security policy, introducing external connections to a secure network is not permitted. This could happen, for example, by connecting a laptop to a nearby unsecured wireless access point while remaining physically connected to the network.

Where remote access to the network is required via a VPN, a request must be made via Everest Engineering's IT service desk. A policy of using two-factor authentication for remote access should be followed in line with the principle of "something you have and something you know" in order to reduce the risk of unauthorised access.

3.6 Supplier remote access to the organisation network

Partner agencies or third party suppliers must not be given details of how to access the organisation's network without permission from the Everest Engineering IT service desk. Any changes to supplier's connections (e.g. on termination of a contract) must be immediately sent to Everest Engineering's IT service desk so that access can be updated or ceased. All permissions and access methods must be controlled by the Everest Engineering IT service desk.

Partners or third party suppliers must contact Everest Engineering's IT service desk to obtain permission for network access on each occasion. All activity logs must be maintained and remote access software and user accounts must be disabled when not in use.

3.7 Review of user access rights

Asset owners must review who has access to the information assets and information processing facilities every 3 months in order to identify:

- people who should no longer have access due to termination or role change;
- user accounts with more access than required by the individual's role;
- user accounts with incorrect role allocations;
- user accounts that do not provide adequate identification such as generic or shared accounts; and
- any other issues that do not comply with this policy.

Reviews must be documented by the asset owner and corrective actions noted.

3.8 User authentication and password policy

All users must:

- not share credentials with any other person;
- not store credentials in clear text (including on paper);
- rotate credentials when there is a possibility of them having been compromised, including accidental exposure; and
- meet minimum password complexity requirements.

Passwords must be:

- minimum length of 16 characters;
- at least one uppercase letter from the Latin alphabet (A-Z);
- at least one lowercase letter from the Latin alphabet (a-z);
- at least one number;
- require at least one non-alphanumeric character (!'@#$%^&*()_+-=[]({}').

Passwords, by themselves, are not sufficient in most cases. Additional authentication methods should be used to minimise the risk of security incidents based on a risk assessment. Single Sign-On (SSO) must be used whenever feasible unless security requirements deem that additional methods are required.

4 System and application access control

Deployment of applications and the design of systems and software must consider how access to the application or system will be controlled. This includes:

- individual user accounts creation processes;
- definition of roles or groups to which user accounts can be assigned;
- allocation of permissions to objects such as files, programs, and menus to subjects (user accounts and groups);
- what views and menu options, and data is visible according to the user account and its permission levels;
- user account administration, including the ability to disable and delete accounts;
- user logon controls such as
  - ensuring passwords are not visible during entry;
  - account lockout once number of incorrect logon attempts exceeds a specified threshold;
  - provide information about number of unsuccessful login attempts and last successful login once user has successfully logged in;
  - date and time-based logon restrictions;
  - device and location logon restrictions; and
  - user inactivity timeout.
- password management such as:
  - ability for user to change password;
  - controls over acceptable passwords; and
  - password expiry.
  - hashed/encrypted password storage and transmission;
- adequate role-based security training is conducted on a regular basis; and
- security auditing facilities, including logon/logoffs, unsuccessful login attempts, object access and account administration activities.

Bespoke software development practices must protect program source code from unauthorised access and modification.

Access to utility programs that provide a method of bypassing system security must be strictly controlled and their use restricted to identified individuals and specific circumstances. Endpoint protection should only allow known penetration testers, for example, to execute their tools of trade on Everest Engineering owner assets.