Everest engineering

Data classification scheme

ISM.10

Version 0.2.3

July 1 2025

Contents

1 Introduction

The Everest Engineering data classification scheme assigns a rating known as a security classification to our information and device assets. It is used for risk identification, to apply appropriate controls to mitigate identified risk, and to determine appropriate lifecycle policies for an information asset or processing facility.

Having a classification scheme also demonstrates to other organisations our commitment to protecting data assets. It is a requirement for many regulatory compliance frameworks.

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 Data security classification

Data security classification is based on the CIA principles triad: confidentiality, integrity, and availability.

The risk of potential harm to the organisation from information is ranked as low, moderate, or high for each of the three principles. Quantifying potential harm requires knowing the intended and authorised use of information and, organisational needs for reliable and timely access.

Impact levels are defined as: limited, serious, and severe or catastrophic. For the purposes of classification, limited impact includes no impact.

The high level security classification process is:

- identify information assets;
- apply classification by confidentiality, integrity and availability; and
- determine the controls appropriate for the information asset based on its security classification.

Note that all information assets need to be tracked in the asset register.

2.1 Impact definitions

We have adopted the definitions from NIST's Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.

A simple scheme is used to assign **low**, **moderate** and **high** ratings to the three security principles for logically or physically separated system components. The impact for an entire system will be the maximum impact rating for each of the three principles. **The single combined impact rating for an entire system will be the highest rating assigned to any of the three principles**.

2.1.1 Low impact

The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- result in minor damage to organizational assets;
- result in minor financial loss; or
- result in minor harm to individuals.

2.1.2 Moderate impact

The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- result in significant damage to organizational assets;
- result in significant financial loss; or
- result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

2.1.3 High impact

The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
- result in major damage to organizational assets;
- result in major financial loss; or
- result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

3 Security labeling

Information assets *and the devices on which they are stored and processed* are either classified or unclassified depending on the assigned impact rating. Note that two possible security labels can be assigned to high impact ratings depending on the potential severity of unauthorised disclosure:

Impact	Security label	Description	Examples
Low	Green - public	**Public**ly available information or information that would be of negligible impact if made public	Product brochures, media releases, company websites or blog posts
Low	Yellow - internal	All **internal** information not released to the public or classified as internal or confidential	Email, wiki pages and information generated in the normal course of normal day to day operations

Impact	Security label	Description	Examples
Moderate	Orange - confidential	**Confidential** information that must be tracked and controlled to prevent unauthorised access or commercially valuable information	Security related information, source code, PII, finance and HR data
High	Red - highly confidential	**Highly confidential** information that if leaked risks significant legal, financial or reputation damage	Unreleased financial information, GDPR defined special data types

All information assets, including documents and general correspondence, is automatically designated as *yellow* unless approved for public release. Information assets of may also be labelled as *orange* or *red*.

Publicly available information whether released by Everest Engineering or sourced from the public domain is typically categorised as unclassified or *green*. When copying or using publicly available information at Everest Engineering only assign it to classified category if there is a business need to do so.

Since the default classification is *yellow*, a public source should be explicitly labeled to avoid confusion.

Note that information designated as green may still require tracking for the purposes of protecting integrity or ensuring availability.

Everest Engineering has specific policies governing the release of information via social media as part of our social media policy. Declassifying information requires approval from the information asset owner and for from our GDPR data controller when personally identifiable information (PII) is involved.

Internal information must always require access to be restricted to an authorised Everest Engineering user account.

Information classified as *orange* or *red* must use network security defence-in-depth techniques to provide additional protection against unauthorised disclosure, modification or loss of availability.