Everest engineering

Backup policy

ISM.13

Version 0.2.3

July 1 2025

Contents

1 Introduction

Update to date, accurate and reliable backups of information and software systems are vital to protect against loss of integrity or availability. This policy defines the requirements for backup plans that information asset owners must develop and implement to adequately protect their assets and software systems.

1.1 Scope

This policy applies to all Everest Engineering information asset owners, including permanent employees, contractors, advisors and contracted partners.

2 Backup policy

Our policy requires backup plans to be created for:

- information we store and process in our day-to-day operation;
- software used to store and process information;
- cloud provider resources; and
- software and system configuration parameters required to operate the system in its entirety.

2.1 Policy requirements

Backup plans must detail compliance with the following:

- backups must be stored in remote locations that are distant enough from the primary processing site to ensure protection against disasters;
- encryption must be used for sensitive information (refer to our data classification scheme);
- encryption keys must be protected against unauthorised use;
- backups must be protected against environmental and human risks (refer to our physical security policy);
- backups must be updated and periodically tested with a frequency appropriate to the criticality of the information;
- backup processes must be monitored for failures with appropriate alerting systems in place; and
- detailed procedures must be documented explaining how systems and information can be restored in the case of partial or complete loss.

In cases where a requirement cannot be met, compensating actions to mitigate risk or a rationale for accepting risk must be documented.

Plans must be recorded in the information asset register and reviewed annually.

2.2 Considerations

Backup plans should consider:

- the type of backup being made (whether full, incremental or differential);
- backup features, their appropriateness and implications. This includes feature such as file-level or block-level backups, compression, and deduplication;
- the required level of redundancy in case a backup is lost, temporarily unavailable or corrupted;
- backup storage – whether on-premises, on remote servers or via cloud service provider resources;
- automation and scheduling;
- regulations affecting the retention and cross-border transfer of PII; and
- who has access to the backed up information and under which circumstances can it be accessed.

2.3 Business continuity planning

Business continuity plans (BCPs) must incorporate backup and recovery plans and be tested as part of disaster recovery scenario testing.