Everest engineering

Incident management procedure

ISM.103

Version 0.2.3

July 1 2025

Contents

1 Introduction

A *security incident* is a *security event* with consequences. Whereas *security events* occur frequently (network scans, brute force password attempts, etc.), an incident is one that has negatively impacted the confidentiality, integrity or availability of our systems.

Examples of incidents include: * network intrusion or improper firewall configuration; * software or configuration changes that introduce vulnerabilities or weaknesses into systems or platforms; * failures in systems or processes to protect information assets; * physical damage to infrastructure, services or system used to secure sites, networks and assets; and * procedural or process gaps that introduce risk or harm to the organisation, assets, systems or staff either through human error or malicious intent.

Security incidents must be reported immediately, regardless of the potential impact or likelihood of damage.

2 Incident response

We use a multidisciplinary team of incident responders to respond quickly and appropriately following our incident and data spill containment checklist.

All security incidents must be evaluated under criteria for notifiable breach obligations. Notifiable breach handling is an Australian legislative requirement to ensure any data breaches such as personally identifiable information (PII) or information that may cause risk or harm to individuals or our commercial partners is investigated and affected parties are notified.

2.1 Raising an incident

Everyone at Everest has an obligation to raise security incidents, including contractors and third parties.

If you are not sure if it is an incident or what the risk is, you must speak with your team lead or line manager immediately or raise the matter as an incident.

The general procedure is to:

- first, notify your manager or team/project lead:
  - if you are onsite and the issue relates to a customers systems, follow their security incident reporting processes
  - don't start your own investigation before opening an incident
    - data breaches and certain types of security incidents have legal implications, evidence collection and any actions taken must follow strict processes
    - accessing or using systems that have been compromised may inadvertently infect other system or compromise evidence
- second, notify the information security team by emailing security@everest.engineering and creating an incident ticket in the Everest Engineering IT service desk.
  - provide clear description of the issue, and why you believe this is a security risk. There are no wrong answers so trust your instincts!
  - do not share details about the incident to anyone except our incident responders;
  - where possible, provide the current status of the issue or risk:
    - is this event or issue still on going?
    - is this risk about something the might happen in the near future?
    - are there indications something happened in the past?

2.2 Incident handling

Breaches of Everest Engineering internal system must be expeditiously handled by:

- triaging the issue to confirm its existence and severity by:

  - evaluating the threat to personally identifiable information(PII) or sensitive data; and
  - determining actions needed to secure all personal identifiable information.
- implement the incident response plan to secure data, systems and staff including:
  - isolating the affected system (depending on severity and criticality);
  - identifying possibilities for short term mitigation and longer term remediation;
  - in consultation with the information security team, applying and testing short term mitigation to restore service;
  - notifying affected individuals and organisations (including customers) of the breach, its severity and possible impact; and
  - remediation through software and system changes.

Refer to our incident response checklist for full overview of incident handling process.

2.3 Who investigates security incidents?

Everest Engineering Incident Responders are members of our security, operations, technology and leadership teams who are trained to assist in the event of a security incident.

By investigating and understanding what or how an event or issue occurred, we can improve our security posture by incorporating any learning or feedback into how we work in the future.

Everest works with many companies and teams to augment their technology capabilities. When we uncover security risks we investigate them regardless of the location or systems owner.

We employ a tiered collaborative approach to disaster and security incident response by following the incident response processes of our customers (where their processes apply) supported by investigation of contributing factors internally through our PIR or incident processes as appropriate.

For any incident that involves assets, processes or services maintained or operated by Everest staff, we must conduct our own investigation following our own incident response process

In all scenarios Everest Engineering will support our customers investigation and incident response processes

- If an event is not within the customers incident response plans, then our internal policies must be adopted even if Everest Engineering systems, services or processes are not impacted
- If the incident may have originated from, or impacted Everest Engineering staff, systems or processes then our internal policies for incident response must be followed in addition to any actions by our customers or third parties
- Incidents originating from or impacting Everest systems, services or processes will be investigated by Everest

All incidents that create risk to personally identifiable information (PII) must be treated as a security incident

2.4 Incident risk and impact assessment

Part of the incident management triage and action plan is to determine the risk posed to the organisation and the urgency of the risk to ensure the appropriate steps are taken.

In receiving an incident, the security team will determine the nature of the threat, whether the threat is ongoing and the potential impact or risk to the organisation.

The security team will assign it an urgency rating based on the nature and response needed using the table below.

Where an incident is not resolved or mitigation or containment is not in place the urgency determines the organisation's immediate response actions to contain and mitigate the incident.

An incident may require follow-up actions that are a lower priority than the initial incident. It is important to capture the initial risk, response and resulting actions even if the incident is later downgraded.

2.4.1 Urgency ranking

Risk mapping	Urgency	Response times	Response resourcing
Critical	Critical	Immediately	Responders team to begin containment
High	Critical	Immediately	Responders team to begin containment
Moderate	Urgent	Within 2 hours	Responders team to begin investigation
Low	Priority	Within 2 business days	Security to action during business hours after triage
Low	Normal	Within normal issue SLA	Security to action as part of security backlog

2.4.2 Risk classification matrix

Risk classification matrix below is used to rank threats, vulnerabilities and incidents by their potential for damage or harm.

The actions taken to contain or mitigate an issue should be assessed using the same risk matrix as the initial incident to ensure steps taken to resolve an open incident to not create new risks.

	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	High	High	High	Critical	Critical
Likely	Moderate	Moderate	High	High	Critical
Possible	Low	Moderate	High	High	Critical
Unlikely, could	Low	Moderate	Moderate	High	High
Rare	Low	Low	Moderate	Moderate	High

Likelihoods are defined as:

- **almost certain**: expected in normal circumstances (100%);
- **likely**: probably occur in most circumstances (10%);
- **possible**: might occur at some time (1%);
- **unlikely**: could occur at some future time (0.1%); and
- **rare**: only in exceptional circumstances (0.01%).

The definitions of potential damage are:

- **insignificant**: no risk to reputation, damage below $1,000 and no PII or information risk;
- **minor**: low risk to reputation, damage below $10,000 with possible PII or information risk;
- **moderate**: low risk to reputation, damage below $100,000 with possible PII or information risk;
- **major**: low risk to reputation, damage below $1,000,000 with possible PII or information risk; and
- **catastrophic**: significant reputation damage, damage above $1,000,000 with possible PII or information risk.

3 Disaster recovery

Production systems critical to business continuity must make use of managed databases and content store services offered by cloud providers whenever possible. These must be configured to operate in high availability mode with redundant nodes for live failover. Different datacenters, or availability zones, must be used for redundant nodes if these are available.

All cloud infrastructure must be managed using code-as-configuration tooling, allowing for rapid recreation of services in the event of a major outage.

If a customer requires a system to operate on unmanaged infrastructure (such as when on-premise) then the system design must incorporate considerations for data redundancy as appropriate for the level of business criticality. These must be clearly described and approved by customers along with plans and procedures for dealing with possible threats (flooding, power outages, structural damage, void & data communication outages, loss of physical access, etc.).