



Incident Response Policy

Draft sample policy — illustrative example prepared for Kranitech Analytics Ltd.

The document is intentionally incomplete and demonstrates the structure and level of detail of a completed policy.

Document	Incident Response Policy	Version	1.0
Organisation	Kranitech Analytics Ltd	Owner	Information Security
Status	Draft	Review cycle	Annual
Classification	Internal	Effective date	Upon approval

1. Purpose

This policy establishes Kranitech Analytics Ltd's approach to identifying, reporting, assessing and responding to information security incidents. It defines the responsibilities required to manage incidents consistently and to support timely recovery and appropriate communication.

2. Organisational context

Kranitech Analytics Ltd does not operate an internal Security Operations Centre (SOC). Security monitoring and related operational support are provided by an external Managed Service Provider (MSP). The MSP supports the organisation in identifying and responding to security events, while Kranitech retains responsibility for business decisions, incident ownership, communications and the management of material impacts.

The MSP's notification and response activities are governed by the applicable service agreement. Where an incident or security event is identified by the MSP, notification to Kranitech shall take place within the service-level timeframes (SLAs) agreed with the provider.

3. Scope

- All information systems, services, data and business processes operated or used by Kranitech Analytics Ltd.
- Security incidents affecting Kranitech, including incidents involving externally provided services or suppliers.
- Employees, contractors and third parties where their activities may contribute to or be affected by an incident.

4. Policy statement

Security incidents shall be reported and managed in a consistent manner. Kranitech shall maintain appropriate arrangements for incident identification, assessment, escalation, response, communication, recovery and post-incident review. The MSP shall support these activities within the responsibilities and SLA commitments defined for the service.



5. Roles and responsibilities

Management

Provides direction, approves material decisions and ensures appropriate resources are available for incident management.

Information Security

Maintains this policy, coordinates incident management, assesses reported incidents and supports escalation and communications.

Employees and contractors

Report suspected incidents promptly and provide relevant information to support assessment and response.

Managed Service Provider (MSP)

Provides monitoring and operational support within the agreed service scope, escalates relevant events to Kranitech and supports response activities when requested or required. The MSP shall meet the incident notification and response SLAs defined in the applicable service agreement.

6. Incident identification and reporting

Potential security incidents may be identified through employee reports, MSP notifications, monitoring activities, customer communications or other credible sources. Suspected incidents shall be reported without unnecessary delay through the designated internal or MSP reporting channel.

6.1 MSP notification

Where an event is identified by the MSP, the MSP shall notify the designated Kranitech contact within the notification SLA agreed for the service. The notification should provide sufficient information to support an initial assessment and should be updated as material facts become available. Kranitech remains responsible for determining the organisational response.

6.2 Internal reporting

Employees and contractors shall report suspected security incidents promptly. Reports should contain the information reasonably available at the time and should not be delayed while attempting to establish the full nature or impact of the event.

7. Incident assessment and classification

Reported events shall be assessed to determine whether they constitute a security incident, the potential business impact, the information or services affected and the level of response required. Classification shall consider factors such as business disruption, confidentiality or integrity concerns, customer impact and regulatory or contractual significance.

7.1 Initial assessment

The initial assessment should establish what is known, what remains uncertain, who needs to be involved and whether immediate protective action is required. Information should be recorded sufficiently to support subsequent review and decision-making.

Illustrative incident classification

Level	Indicative impact	Response expectation
High	Material business or customer impact	Immediate escalation and coordinated response.
Medium	Limited but meaningful impact	Prompt assessment, containment and management oversight.
Low	Limited impact with no material disruption	Routine handling and review.



8. Incident response

8.1 Containment

Immediate actions shall be taken where necessary to limit further impact, protect relevant information or services and preserve the ability to investigate the incident.

8.2 Investigation and analysis

Relevant information shall be gathered and assessed to establish the nature, scope and likely cause of the incident. The level of investigation shall reflect the circumstances and business impact.

8.3 Recovery

Affected services shall be restored in a controlled manner, with appropriate checks to confirm that recovery actions have addressed the identified impact.

8.4 Communication

Incident communications shall be coordinated according to the nature and significance of the incident. Internal stakeholders, customers, suppliers and other parties shall be informed where appropriate.

9. External and regulatory notification

Where an incident may trigger contractual, regulatory or other external notification obligations, the relevant requirements shall be assessed and the appropriate notification route agreed by the responsible Kranitech function. Where the incident involves an MSP or other service provider, the contractual notification SLA shall also be considered and the provider's notification record retained.

10. Evidence and record keeping

Incident records shall contain sufficient information to support management decisions, follow-up actions and subsequent review. Relevant evidence shall be retained in accordance with Kranitech's information retention requirements and any applicable contractual obligations.

11. Post-incident review

Material incidents shall be reviewed after response activities have been completed. The review shall consider the effectiveness of the response, lessons identified, required improvements and whether changes to controls, procedures or supplier arrangements are appropriate.

12. Testing and exercising

Incident response arrangements shall be tested periodically using appropriate exercises or other validation activities. Findings shall be recorded and used to improve the organisation's readiness.

13. Third-party and MSP management

Responsibilities for incident management involving the MSP or other relevant third parties shall be defined through applicable service and contractual arrangements. Material changes to the services, notification SLAs or responsibilities shall be reflected in the relevant documentation.

14. Policy exceptions

Exceptions to this policy shall be documented, justified and approved by the appropriate authority.



15. Compliance and monitoring

Compliance with this policy shall be monitored through appropriate management review, incident records, response exercises and other assurance activities. Significant non-compliance or recurring weaknesses shall be addressed through appropriate corrective actions.

16. Policy review

This policy shall be reviewed at least annually and following significant changes to the organisation, its services, its incident management arrangements, its MSP relationship or relevant requirements.

Appendix A – Incident classification

The following classification model is illustrative. The final thresholds and escalation criteria would be confirmed as part of the agreed policy scope.

Level	Typical trigger	Escalation
High	Material impact or significant external effect	Management and Information Security immediately; coordinated MSP support.
Medium	Meaningful but contained impact	Information Security review and management awareness.
Low	Limited impact	Routine handling with appropriate recording.

Appendix B – Incident reporting contacts

The final policy would include the current internal and MSP reporting routes, responsible contacts and escalation details. These details are intentionally omitted from this sample.

Sample completion note

This sample intentionally omits detailed procedures, contact details and operational thresholds that would be completed for the agreed requirements and organisation context.