

VERSION 2.2 · FINAL

Incident Response Policy

How EthicSuite detects, responds to and recovers from security incidents

Document ID	ES-POL-005
Version	2.2
Status	Final
Classification	Internal
Policy owner	Information Security Officer
Approved by	Justin Veeran, Chief Executive Officer, on behalf of the Board of Directors of Ethics Helpdesk (Pty) Ltd
Policy period	28 February 2026 – 1 March 2027
Effective date	28 February 2026
Next review	1 March 2027

Approval

Signature	
Name	Justin Veeran
Title	Chief Executive Officer, Ethics Helpdesk (Pty) Ltd
Date	28 February 2026

Version history

Version	Date	Change
2.2	28 February 2026	Current issue, valid 28 February 2026 – 1 March 2027

1. Purpose

This policy sets out how EthicSuite detects, responds to, recovers from and learns from information security incidents, so that harm to tenants and reporters is minimised and legal notification duties are met.

2. Scope

This policy applies to all incidents affecting EthicSuite systems, data or suppliers, including incidents at sub-processors that affect EthicSuite or tenant data. It aligns with NIST SP 800-61 (Rev. 3) and ISO/IEC 27035.

3. Definitions

Term	Meaning
Security event	An observed occurrence that may indicate a security issue (e.g. a failed login spike).
Security incident	An event that actually or probably compromises the confidentiality, integrity or availability of information or systems.
Security compromise (POPIA)	Reasonable grounds to believe personal information has been accessed or acquired by an unauthorised person (POPIA s22).
Material incident	An incident classified as Critical or High under section 4.

4. Incident Classification

Incidents are classified by severity as follows:

Severity	Examples	Respond within	Contain / recover target
SEV1 Critical	Exposure of reporter identity or vault data; ransomware; confirmed breach across tenants; full platform outage	15 minutes, 24/7	Contain within 4 hours; restore service within 24 hours (RTO)
SEV2 High	Confirmed breach of one tenant's data; compromised privileged account; major service degradation	1 hour, 24/7	Contain within 8 hours; resolve within 48 hours
SEV3 Medium	Malware on a single endpoint; limited misdirected disclosure; exploitable vulnerability with no evidence of use	4 business hours	Resolve within 5 working days
SEV4 Low	Blocked phishing attempt; policy breach with no data impact	1 business day	Resolve within 10 working days

When in doubt, an incident is classified at the higher level and downgraded later.

5. Incident Response Team and Escalation

Role	Responsibility
Incident Commander	Leads the response, decides priorities and keeps the timeline. Normally the Information Security Officer, unless the CEO appoints someone else.
Technical Lead	Investigation, containment, eradication and recovery. Normally the senior engineering lead.
Information Officer	Assesses POPIA impact and manages regulator and data subject notifications. Justin Veeran (CEO), or a deputy he designates.
Communications Lead	Tenant and external communications. Appointed by the CEO for each incident.
Legal Counsel	Legal advice, evidence handling and law enforcement liaison. Internal or external counsel appointed by the CEO.
Executive Sponsor	Decisions on business impact and Board escalation. The Chief Executive Officer.

SEV1 incidents are escalated to the Executive Sponsor immediately and to the Board within 4 hours; SEV2 incidents within 24 hours. The Information Security Officer maintains a 24/7 incident contact, which is communicated to all personnel and to tenants.

6. Response Lifecycle

Phase	Key actions
1. Prepare	Keep this policy, playbooks (ransomware, data breach, account takeover, DDoS, insider), contact lists and tools current; train the team.
2. Detect and report	All personnel and systems report suspected incidents immediately. Tenants report through support; security researchers through the contact channels published on the EthicSuite website.
3. Triage	Confirm the incident, classify severity, open an incident record and assemble the team.
4. Contain	Limit the damage — isolate systems, disable compromised accounts, rotate keys and credentials.
5. Eradicate	Remove the root cause — malware, vulnerabilities, unauthorised access.
6. Recover	Restore from clean backups, verify integrity, monitor closely for recurrence.
7. Learn	Post-incident review, corrective actions and policy updates (section 10).

7. Evidence Handling

Evidence (logs, images, disk snapshots) is preserved and handled with a documented chain of custody so it can be used in disciplinary, civil or criminal proceedings. Personnel must not investigate on their own or tamper with affected systems before the Technical Lead gives instructions.

In a ransomware incident, EthicSuite will not pay a ransom as long as it can recover from backups; any payment decision is reserved for the Board after legal advice.

8. Notification Requirements

Affected tenants and, where required by law, regulators are notified as follows:

Who	When	Basis / notes
Affected tenants	Without undue delay and within 24 hours of reasonable grounds to believe their data is affected; updates every 24 hours until resolved	POPIA s21(2) (operator duty); tenant agreements
Information Regulator	As soon as reasonably possible — target 72 hours — via the eServices portal	POPIA s22, where EthicsSuite is responsible party. No minimum threshold; initial report may be updated as facts emerge
Affected data subjects	As soon as reasonably possible	POPIA s22(4)–(5); the tenant usually notifies for case data, with EthicsSuite's support
South African Police Service	Within 72 hours of becoming aware, where the law applies	Cybercrimes Act s54 (once in force and if applicable to EthicsSuite)
Tenants that are financial institutions	Support provided quickly enough for them to meet their 24-hour regulator notification	FSCA/PA Joint Standard 2 of 2024
Board of Directors	SEV1 within 4 hours; SEV2 within 24 hours	Governance oversight

Notifications are only delayed where the police or the Information Regulator determine that notice would impede a criminal investigation.

9. Communications

Only the Communications Lead, with Executive Sponsor approval, may make statements to tenants, the media or the public about an incident. Communications must never reveal information that could identify a reporter.

10. Post-Incident Review

A blameless post-incident review is completed within 10 working days of closing every SEV1 and SEV2 incident (and SEV3 where useful). It records the timeline, root cause, what worked, what did not, and corrective actions with owners and due dates, which are tracked to completion.

11. Testing and Training

The incident response plan is tested through a tabletop exercise at least annually, including a reporter-data breach scenario and a ransomware scenario. Incident response team members are trained on joining and after each exercise.

12. Records

All incidents, including those not reportable to regulators, are recorded in the incident register and retained for 5 years.

13. Policy Review

This policy is reviewed at least annually, after every SEV1 incident, and after each test.