

VERSION 2.2 · FINAL

Information Security Policy

Protecting the confidentiality, integrity and availability of tenant and reporter information

Document ID	ES-POL-001
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 EthicSuite's approach to protecting the confidentiality, integrity and availability of information processed by the EthicSuite™ platform, including tenant data and the identity of whistle-blowers and reporters. It is the parent policy for the Access Control, Data Protection (POPIA), Data Retention and Incident Response policies.

Because EthicSuite handles ethics reports, protecting **reporter anonymity** is treated as the highest-priority security objective across every control in this policy.

2. Scope

This policy applies to:

- all EthicSuite and Ethics Helpdesk (Pty) Ltd directors, employees, temporary staff, contractors and consultants;
- all third-party service providers (operators and sub-processors) that store, process or access EthicSuite information;
- all environments (production, staging, development, backup and disaster recovery), endpoints, source code, cloud accounts and supporting tools;
- information in every format — electronic, paper and verbal.

3. Policy Statement and Framework Alignment

EthicSuite manages information security through a risk-based Information Security Management System (ISMS). The ISMS is aligned with:

- ISO/IEC 27001:2022 and ISO/IEC 27002:2022 (control set);
- NIST Cybersecurity Framework 2.0 and CIS Critical Security Controls v8;
- the Protection of Personal Information Act 4 of 2013 (POPIA), section 19 (security safeguards);
- the Cybercrimes Act 19 of 2020, the Protected Disclosures Act 26 of 2000 and the Electronic Communications and Transactions Act 25 of 2002;
- the King IV™ Code on Corporate Governance (governance of technology and information).

EthicSuite aims to achieve independent ISO/IEC 27001 certification within 18 months of this policy's approval. Where tenants are financial institutions subject to FSCA/Prudential Authority Joint Standard 2 of 2024 (Cybersecurity and Cyber Resilience), EthicSuite will support their obligations through its contracts and controls.

4. Governance, Roles and Responsibilities

Role	Responsibility
Board of Directors, Ethics Helpdesk (Pty) Ltd	Ultimately accountable for information security. Approves this policy annually and receives security reporting quarterly.
Information Security Officer (ISO)	Designated in writing by the Chief Executive Officer. Owns this policy and the ISMS, maintains the risk register, approves exceptions and leads incident response.
Information Officer (POPIA)	Registered with the Information Regulator. Ensures POPIA compliance, handles data subject requests and regulator notifications.

Role	Responsibility
Engineering and DevOps lead	Implements technical controls, secure development, change management, patching and backups.
Super Admins	Administer the platform in line with the Access Control Policy; hold the most privileged access and are subject to enhanced monitoring.
All personnel	Comply with this policy, complete training and report suspected incidents immediately.
Third parties	Meet security requirements equivalent to this policy, as set out in their contracts.

5. Risk Management

Information security risks are identified, assessed and treated using a documented methodology. The risk register is reviewed quarterly and whenever there is a material change to the platform, a new vendor or a significant incident. Residual risks above the agreed appetite must be accepted in writing by an executive director.

6. Information Classification and Asset Management

All information is classified by its owner using the scheme below, and handled according to its classification:

Level	Examples	Minimum handling
Restricted	Reporter identity and vault data, evidence files, voice recordings, encryption keys, credentials	Field-level encryption, dual-approval access, full audit trail, never exported to personal devices
Confidential	Case data, investigation notes, tenant configuration, personal information, contracts	Encrypted at rest and in transit, role-based access, logged access
Internal	Policies, internal procedures, architecture documents	Access limited to personnel and approved third parties
Public	Marketing material, published policies, PAIA manual	Approved before release

An inventory of information assets (systems, data stores, cloud accounts, endpoints and key vendors) is maintained, each with a named owner, and reviewed quarterly.

7. Access Control

Access is granted on a least-privilege, need-to-know, role-based basis, with multi-factor authentication (MFA) for all workforce access and all privileged tenant roles. Full requirements are set out in the Access Control Policy (ES-POL-002).

8. Cryptography and Key Management

- Data in transit is encrypted using TLS 1.2 as a minimum, with TLS 1.3 preferred; weak ciphers and protocols (SSL, TLS 1.0/1.1) disabled; HSTS enabled.
- Data at rest is encrypted using AES-256 (or equivalent) for all databases, file stores and backups.

- Restricted data (reporter vault, evidence and recordings) is additionally protected by application or field-level encryption with separate keys per tenant.
- Keys are held in a managed key management service or hardware security module, never in source code, and rotated at least annually and immediately on suspected compromise.
- Secrets (API keys, passwords, tokens) are stored only in an approved secrets manager.

9. Secure Development and Change Management

- Security is built into the software development lifecycle, following OWASP Top 10 and OWASP ASVS guidance.
- Every code change is peer-reviewed before merge; no developer may approve their own change to production.
- Automated static analysis (SAST), dependency/software-composition scanning and secret scanning run on every build; critical findings block release.
- Production, staging and development environments are separated. Real tenant or reporter data is never used in development or testing.
- Production changes follow an approved change process with rollback plans; emergency changes are reviewed retrospectively within 2 working days.
- New features that touch Restricted data require a security and privacy review before release.

10. Vulnerability and Patch Management

Vulnerability scanning is performed continuously for code dependencies and containers, and at least weekly for infrastructure and external-facing services. Independent penetration testing is performed at least annually and after any major architectural change, and results are shared with tenants in summary on request.

Security patches are applied within the following timeframes from release or discovery:

Severity (CVSS)	Target timeframe	Notes
Critical (9.0–10) or actively exploited	72 hours	Emergency change process may be used
High (7.0–8.9)	14 days	
Medium (4.0–6.9)	30 days	
Low (0.1–3.9)	90 days or next scheduled release	

Where a patch cannot be applied in time, compensating controls must be put in place and an exception recorded.

11. Security Monitoring and Logging

- Security-relevant events (authentication, privileged actions, access to Restricted data, configuration changes, admin actions and API errors) are logged centrally.
- Logs are protected against tampering, time-synchronised, and retained for 12 months, with at least 90 days immediately searchable.
- Security alerts are monitored 24/7 through automated alerting; critical alerts are acknowledged within 1 hour and all other alerts are triaged at least daily.
- Threat intelligence feeds are used to update detection rules and patching priorities.

12. Backup, Business Continuity and Disaster Recovery

- Backups are taken at least daily, encrypted, and stored in a separate location and account from production, with immutability enabled so they cannot be altered or deleted by ransomware.
- No person with routine production access has delete rights over backups.
- Restores are tested quarterly; a full disaster recovery test is carried out annually.
- Recovery objectives for the core platform: Recovery Point Objective (RPO) 24 hours and Recovery Time Objective (RTO) 24 hours.
- A business continuity plan covering key people, suppliers and communications is maintained and tested annually.

13. Endpoint, Network and Cloud Security

- All devices used to access EthicSuite systems are company-managed or enrolled in device management, with full-disk encryption, endpoint detection and response (EDR), automatic screen lock and current patches.
- Production networks are segmented; administrative interfaces are not exposed to the public internet.
- Internet-facing services are protected by a web application firewall and DDoS protection.
- Cloud configurations are continuously checked against a secure baseline (e.g. CIS Benchmarks).

14. Third-Party and Vendor Risk Management

EthicSuite remains accountable for information processed by its suppliers. Before onboarding, every supplier that will access EthicSuite information is assessed for security posture and POPIA compliance (e.g. ISO 27001 or SOC 2 report, security questionnaire). Critical suppliers are reassessed annually and others every two years.

Supplier contracts must include confidentiality, security and breach-notification obligations, POPIA operator terms (sections 20 and 21), a right to audit, and return or deletion of data on termination. A current list of sub-processors is made available to tenants.

15. People Security and Awareness

- Background checks are carried out for roles with access to Confidential or Restricted data, where lawful and proportionate.
- All personnel sign confidentiality undertakings before receiving access.
- Security and POPIA training is completed on joining and annually thereafter; completion is tracked.
- Phishing simulations are run at least quarterly.

16. Artificial Intelligence and Automated Tools

AI tools and models may only process EthicSuite or tenant information if approved by the ISO and Information Officer. Tenant and reporter data must never be used to train third-party models without the tenant's written agreement, and AI-assisted outputs affecting case outcomes must be reviewed by a person.

17. Incident Management

All personnel must report suspected security incidents immediately to the Information Security Officer through EthicSuite's designated security reporting channel. Incidents are handled under the Incident Response Policy (ES-POL-005).

18. Compliance, Monitoring and Measurement

Compliance with this policy is monitored through automated controls, internal reviews and an annual internal audit. Key metrics (for example patch compliance, MFA coverage, open high-risk findings, training completion and incident counts) are reported to the Board quarterly.

19. Exceptions and Non-compliance

Exceptions

Any exception to this policy must be requested in writing, state the business reason and compensating controls, and be risk-accepted by the Information Security Officer. Exceptions are time-bound to a maximum of 6 months, recorded in the exceptions register, and re-approved before expiry.

Non-compliance

Breach of this policy may lead to disciplinary action in line with EthicSuite's disciplinary code, up to and including dismissal, and to termination of contracts for contractors and third parties. Where a breach may constitute an offence (for example under the Cybercrimes Act 19 of 2020 or POPIA), EthicSuite may refer the matter to the relevant authorities.

20. Related Documents

- Access Control Policy (ES-POL-002)
- Data Protection / POPIA Policy (ES-POL-003)
- Data Retention Policy (ES-POL-004)
- Incident Response Policy (ES-POL-005)
- Business Continuity and Disaster Recovery Plan
- PAIA Manual

21. Policy Review

This policy is reviewed at least annually, or sooner following a material change to the platform, the threat landscape, the law or after a significant incident.