

VERSION 2.2 · FINAL

Access Control Policy

How access to EthicSuite systems and data is granted, reviewed and revoked

Document ID	ES-POL-002
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 governs how access to EthicSuite systems and data is requested, approved, authenticated, reviewed and revoked, so that only the right people have the right access for the right length of time.

2. Scope

This policy covers:

- **workforce access** — employees, contractors and suppliers accessing EthicSuite infrastructure, cloud consoles, source code, internal tools and support systems;
- **platform access** — tenant users (administrators, case managers, investigators, reporters) accessing the EthicSuite application;
- **machine access** — service accounts, API keys and integrations.

Tenants manage their own users within the platform, but EthicSuite enforces the minimum platform controls set out in this policy.

3. Access Control Principles

- **Least privilege** — access is granted strictly on the basis of role and operational need, and no broader.
- **Need to know** — access to case and reporter information is limited to people working on that matter.
- **Default deny** — anything not explicitly allowed is blocked.
- **Segregation of duties** — no single person can request, approve and implement their own privileged access or production change.
- **Unique identity** — every user has their own account; shared or generic accounts are not permitted.
- **Role-based access (RBAC)** — access is assigned through defined roles, not to individuals ad hoc.

4. Access Requests and Approval

Workforce access is requested through a recorded ticket and approved by the person's line manager and the system owner before it is granted. Access to Restricted data (reporter vault, evidence and recordings) additionally requires approval by the Information Security Officer and the Information Officer.

5. Authentication and Multi-Factor Authentication

MFA is mandatory for:

- all workforce access to production, cloud consoles, source code repositories, email and collaboration tools, and the EthicSuite admin panel;
- all tenant users with administrator, case manager or investigator roles — this cannot be switched off by tenants;
- all remote access and all third-party access.

Approved MFA methods are phishing-resistant methods (FIDO2 security keys or passkeys) for privileged users; authenticator app push or time-based codes for other users. SMS codes are not permitted for privileged access. Single sign-on (SSO) through the tenant's identity provider is supported and encouraged.

Anonymous reporters are not required to create accounts. Reporter follow-up access uses a system-generated case key and a reporter-chosen password, protected by rate limiting, so that anonymity is preserved.

6. Password Requirements

Password requirements follow NIST SP 800-63B guidance:

- minimum length of 12 characters for standard users and 14 characters for privileged users, with long passphrases encouraged;
- new passwords are checked against lists of known breached and common passwords;
- no forced periodic rotation — passwords are changed immediately when compromise is suspected;
- accounts are temporarily locked after 10 consecutive failed attempts, with rate limiting on all login endpoints;
- workforce users must use the company-approved password manager;
- passwords are stored only as salted hashes using a strong, slow algorithm (e.g. Argon2id or bcrypt).

7. Session Management

Sessions time out after 15 minutes of inactivity for admin, case manager and investigator roles, and 30 minutes for other users, with an absolute maximum session length of 12 hours. Sessions are invalidated on logout, password change and role change.

8. Privileged Access

Access to privileged and administrative functions is limited to:

- named individuals approved by the Information Security Officer, with the number of Super Admins kept to the minimum needed to run the platform;
- separate admin accounts, distinct from day-to-day accounts;
- just-in-time elevation that expires automatically, rather than standing admin rights, wherever the platform supports it;
- full logging of all privileged sessions and actions, reviewed by someone other than the admin.

Emergency (break-glass) accounts are sealed, protected by MFA, used only in an emergency and reviewed after each use.

9. Reporter Anonymity and Tenant Data Segregation

- No EthicsSuite employee has routine access to reporter vault contents. Access is only possible through a break-glass process with dual approval and is disclosed to the affected tenant.
- Each tenant's data is logically isolated; isolation is tested on every release.
- EthicsSuite support staff may access tenant data only with the tenant's documented permission, for a limited time, and every access is logged and visible to the tenant.
- Platform logs must not record data that could identify an anonymous reporter (for example IP addresses on anonymous channels).

10. Access Reviews

User access rights are reviewed as follows:

Access type	Review frequency
Privileged and Super Admin access	Quarterly
Access to Restricted data	Quarterly

Access type	Review frequency
All other workforce access	Every six months
Third-party and vendor access	Quarterly
Tenant users	Tenants receive a user-access report quarterly to review their own users

Reviews are signed off by the system owner; access that is no longer needed is removed within 5 working days of the review.

11. Joiners, Movers and Leavers

- **Joiners** — access is provisioned only after a signed confidentiality agreement and approval.
- **Movers** — access no longer needed for the new role is removed within 5 working days of the role change.
- **Leavers** — all access is revoked within 24 hours of departure; for dismissals or privileged users, access is revoked immediately, before or at the time the person is informed.
- Devices, keys and tokens are returned and recorded on exit.
- Accounts inactive for 90 days are automatically disabled.

12. Third-Party and Remote Access

Third-party access must have an internal sponsor, be limited in time and scope, use MFA and be logged. Remote access to production is only through approved, encrypted channels from managed devices.

13. Service Accounts and API Keys

Every service account and API key has a named owner, the minimum permissions required, is stored in the secrets manager and rotated at least annually and immediately when a person with knowledge of it leaves. Service accounts cannot be used for interactive login.

14. Monitoring

Failed logins, unusual access patterns, access to Restricted data and privilege changes are logged and generate alerts in line with the Information Security Policy.

15. 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.

16. Related Documents and Review

This policy supports the Information Security Policy (ES-POL-001) and the Incident Response Policy (ES-POL-005). It is reviewed at least annually or following a material change.