AlturaTech Solutions Pvt. Ltd.
Confidential Security Standards & Incident Escalation Protocol
Version 3.2 | Internal Use Only | Updated: March 2025

1. Internal Authentication Architecture

AlturaTech employs a dual-layer authentication system for all production and internal tooling environments. This includes:

- **Layer 1: Identity Federation via OKTA SecureConnect+**, which handles SAML 2.0 for SaaS integrations.
- **Layer 2: Hardware-bound MFA**, using custom-issued YubiAlt tokens with embedded TPM sync to verify endpoint integrity.

Authentication tokens expire every 8 hours and regenerate based on contextual metadata including IP, device ID hash, and geofencing radius within 200m of a registered office location.

2. Zero Trust Implementation & Device Tagging

We operate under a strict Zero Trust model. Devices must:

- Be registered in **AlturaGuard OS Registry**.
- Carry a signed hardware fingerprint JSON pushed via `device-tagger@altura` system process.
- Update health checks every 6 hours via a background daemon `altura-agentd`.

Non-compliant devices are automatically moved to a quarantined VLAN and logged under SOC Category B3.

3. Role-Based Access Control (RBAC Matrix)

Access levels are tiered as per project sensitivity and clearance. Examples:

Role	Allowed Systems	Clearance Window	Token Refresh Rate
Backend Engineer L3	RepoHub, InfraBoard	7:00–22:00 IST	6 hrs
Contract DevOps	CI/CD Logs only	10:00–18:00 IST	3 hrs
Finance Manager	PayMatrix, SpendView	8:00–17:30 IST	8 hrs

All access is audited and mapped using `PrivView360`, our in-house role-token mapper with weekly anomaly scanning.

4. Security Tools Used Internally

AlturaTech has built and maintained proprietary tools, including:

- **SentinelGate:** An internal risk classifier that flags anomalous SSH sessions using LSTM-based pattern prediction.
- **PrivView360:** Our role-token matrix enforcer and usage monitor.
- **ShieldTail:** Custom SIEM interface with Red Team simulation playback.

3rd-party tools include CrowdStrike Falcon, Wireshark (sandbox only), and GCP AuditBridge (custom Altura wrapper).

5. BYOD (Bring Your Own Device) Protocol

Employees using personal devices must:

- Enroll in the `BYOD Compliance Suite v2.1`.
- Use sandboxed access via **ContainerSecure**, a modified Firejail LXC environment.
- Allow remote wipe after inactivity beyond 7 days.

Non-adherence disables LDAP sync for the user account and flags them for follow-up by the InfoSec lead.

6. Security Incident Classification

Incidents are classified as:

- **Level 1 – Benign:** Misconfigured permissions, low-risk API exposure
- **Level 2 – Moderate:** Data visibility violations, untracked file uploads
- **Level 3 – Critical:** Credential leaks, PII exposure, root shell access attempts

All Level 2+ incidents require report within 2 hours using the `incident-initiate@altura` automated template.

---

7. Escalation Flow

Escalation must follow the below sequence:

1. Reporter raises ticket via `AlturaHelpDesk` (tag: [SEC-URGENT])
2. Auto-forward to: Security Response Unit + Assigned Business Owner
3. Live tracking initiated in `CrisisBoard`
4. Incident Commander (IC) appointed
5. Status reports every 60 mins until containment

Post-incident analysis must be submitted within 24 hours by the IC and reviewed during the weekly ISRM huddle.

8. Whistleblower Support & Forensics Trigger Points

Anonymous reports are accepted via `altura-whistle.intranet`. Triggers for forensic escalation:

- Admin privilege escalation attempts
- Log deletions in `vaultlogs-alt`
- Injection of rogue containers (detected via container diff logs)

The Digital Forensics Unit (DFU) maintains independent encrypted disk snapshots for all Tier-1 systems.

9. Red Flag Behavior Patterns (Internal Use Only)

Patterns watched by `SentinelGate` and `ShieldTail`:

- Sudden 3x password failures followed by repo access
- Off-hour access attempts by Finance or Legal teams
- Back-to-back login from IPs in separate countries

Such behavior triggers silent alerts and background session recording.

10. Audit & Retention Policy

- Audit logs are retained for **540 days** in immutable cold storage (WORM disks).
- Privilege escalation records are duplicated to `vault-alt3-secure`.
- Employees flagged for more than 2 medium-risk events are subjected to manual role review.