IT
CORPORATE SECURITY POLICY

Policy Code: TA-SEC-POL-01

Table of Contents

This policy defines the minimum-security measures required at Tech Aura to ensure the protection of its people, physical premises, IT infrastructure, and confidential assets. It supports regulatory compliance (ISO 27001) and builds a secure operational environment.

1. Definitions

- **Risk Management:** Identifying and mitigating organizational threats through proactive planning.
- **Emergency Response:** Coordinated plan to respond to incidents impacting people or operations.
- **Security Training:** Instruction for employees on safe practices and incident response.
- **Critical Area:** Site, system, or function that is essential to operational continuity.
- **Confidential Information:** Data or information that must be protected against unauthorized access.
- **Threat:** A potential cause of an unwanted incident that may result in harm.
- **Incident Response:** Structured approach to handle and recover from security events.
- **Access Control:** Measures to limit access to resources based on identity and need.

2. Key Elements and Responsibilities

Chief Executive Officer

- Approves this policy and strategic security actions.
- Leads crisis and emergency teams.
- Decides on high-severity cases.

QHSE Manager / Security Officer

- Develops and implements the security program.
- Conducts corporate risk assessments.
- Leads emergency and crisis coordination.
- Reviews and signs security documentation.
- Maintains incident records and logs.
- Coordinates internal security audits.

HR & Finance Officer

- Disseminates alerts and updates to staff.
- Coordinates staff training compliance.
- Maintains training participation records.
- Ensures security onboarding is conducted for new hires.

Country/Department Managers

- Apply and enforce the policy locally.
- Ensure training, equipment, and emergency awareness is active.
- Report incidents and suspicious activity to the QHSE Manager.
- Organize fire drills and briefings.

3. Security Frameworks

An internal alert system shall be used to quickly inform employees of threats or security concerns.

- An internal alert system shall be used to quickly inform employees of threats or security concerns.
- Risk levels (Low, Medium, High, Critical) must be defined.
- Action plans for each level must be prepared in advance.
- Key contacts must be notified during high or critical alerts.
- The alert management protocol must be tested annually.
- Alerts must be sent using approved channels (email, phone, SMS, loudspeaker).
- Regular simulation drills must be documented.

3.1. Fire Prevention

Issue: Fire or disaster causing physical damage and data loss.

Resolution:

• Evacuation plans posted throughout the premises.

•Fire extinguishers, alarms, and smoke detectors tested quarterly.

• Server rooms marked on all floor plans.

• Fire Marshals designated per site.

• Mandatory fire safety training annually.

3.2. Access Control

Issue: Unauthorized physical access to secure areas.

Resolution:

• Access only for authorized personnel.

• Visitor entry is documented daily.
• Badge or biometric systems are recommended.
• Access permissions based on job role.
• Real-time occupancy tracked through logs or digital systems.

3.3. Security Awareness Training

Issue: Employees falling victim to phishing or mishandling data.
Resolution:
• Annual security training for all staff.
• Quarterly training for high-risk roles.
• Topics include phishing, malware, social engineering, and evacuation.
• Onboarding training completed within 2 weeks of joining.
• HR retains training logs for auditing.

3.4. Malware & Virus Protection

Issue: Malware infections from email, downloads, or external devices.
Resolution:
• Antivirus installed on all endpoints with real-time protection.
• Definitions updated daily.
• Email links and attachments scanned.
• USB device usage restricted to approved devices only.
• Full scans performed weekly.

3.5. Phishing & Social Engineering

Issue: Employees being tricked into revealing sensitive info.
Resolution:
• Simulated phishing tests conducted quarterly.
• Staff trained to verify unknown callers or requests.
• No credentials or sensitive data shared without validation.
• IT helpdesk available for reporting.

3.6. Unauthorized Access & Hacking Attempts

Issue: Hackers gaining access via weak passwords or system loopholes.
Resolution:

- Multi-Factor Authentication (MFA) enabled on all logins.
- Strong password policies (12+ characters, no reuse).
- Firewall and IDS/IPS systems actively monitored.
- Account lockout after failed attempts.

3.7. Ransomware Threats

Issue: Ransomware locking data and halting operations.

Resolution:

- Backups performed daily and stored offline.
- Admin rights limited to essential users.
- Backup restoration tested monthly.
- Staff trained to avoid suspicious links/files.

3.8. Data Breaches & Data Loss

Issue: Exposure or accidental deletion of sensitive data.

Resolution:

- Data encrypted during storage and transfer.
- Only authorized roles can access sensitive info.
- Breach response team responds within 24 hours.
- System and access logs regularly reviewed.

3.9. Insecure Remote Access

Issue: Remote work causing security loopholes.

Resolution:

- VPN use required for all remote users.
- Remote devices must meet endpoint security standards.
- MFA enforced on all cloud and remote systems.
- Remote access logs monitored weekly.

3.10. Unpatched Systems & Software Vulnerabilities

Issue: Exploits due to outdated systems.

Resolution:

- OS and app updates auto-installed.
- Critical patches applied within 48 hours.
- Monthly vulnerability scans.
- Deprecated software is removed or sandboxed.

3.11. Insider Threats

Issue: Data leaks or sabotage by internal staff.

Resolution:

- Role-based access control for all systems.
- Signed confidentiality and usage policies for all staff.
- Real-time user activity logging.
- Immediate revocation of access upon exit.

3.12. Incident Response Management

Issue: Unstructured or delayed incident handling.

Resolution:

- Incident Response Plan in place with clear roles.
- Phases: Identify → Contain → Eradicate → Recover → Report.
- Incident drills every 6 months.
- Incidents are logged and analysed for improvements.

3.13. DDoS (Distributed Denial of Service) Attacks

Issue: Flood of traffic crashing company servers or websites.

Resolution:

- Cloud-based DDoS protection enabled (e.g., AWS Shield, Cloudflare).
- Rate-limiting rules applied at the firewall level.
- Real-time network monitoring for traffic anomalies.
- Immediate escalation protocol for large-scale attacks.

3.14. Cloud Security Misconfiguration

Issue: Exposed databases or resources in cloud services.

Resolution:

- Admin access restricted and MFA enforced.
- Cloud storage (e.g., Google Drive, AWS S3) must be encrypted.
- Cloud configurations are reviewed quarterly.
- Logs are enabled for all cloud activity.

3.15. Third-Party & Vendor Risk

Issue: Security breaches caused by vendors or partners.

Resolution:

- All vendors must sign a Data Protection Agreement (DPA).
- Third-party access reviewed monthly.
- Vendors with access must comply with our security controls.
- Risk assessments conducted before onboarding vendors.

4. Reference Documents

This policy aligns with the following foundational documents that define core frameworks, regulatory expectations, and risk preparedness practices applicable to Tech Aura:

Document Title	Purpose
ISO/IEC 27001 Control Requirements	International standard for establishing, maintaining, and improving an ISMS.
Business Continuity Plan (BCP)	Outlines contingency strategies to ensure continuous business operations.
Company Risk Register	Catalogues identified organizational risks with their impact and mitigation status.

Related Documents

The following internal procedural documents support the operationalization of this policy:

Document Code	Title	Description
PRO-SEC-01	Fire Prevention Procedure	Protocol for fire risk reduction and emergency readiness.
PRO-SEC-02	Access Control Guidelines	Defines role-based access rules for physical and digital areas.
PRO-SEC-03	Emergency Response Procedures	Action plans for responding to various emergency scenarios.
PRO-TRAIN-01	Security Awareness Training Plan	Curriculum for staff security and compliance education.

5. Related Quality System Records

Below records are maintained as verifiable evidence of control implementation and compliance:

Record Code	Record Title	Purpose
FOR-SEC-01	Fire Drill Completion Log	Logs fire drill execution, participation, and observations.
FOR-SEC-02	Access Badge Assignment Form	Tracks badge issuance, deactivation, and access privileges.

FOR-SEC-03	Security Incident Report Form	Used to report and analyze security breaches or near misses.
FOR-SEC-04	Emergency Response Checklist	Verifies completion of required actions during an emergency.

6. Appendices

This section includes supplemental materials referenced in the document, such as evacuation maps, floor plans, policy flowcharts, compliance checklists, training attendance sheets, and regulatory cross-reference indexes. These items are maintained by the QHSE department and reviewed during policy audits.

Reviewed By: Chief Executive Officer

Date: [04/06/25]

All revisions must be reviewed and approved by the Chief Executive Officer