Corporate Security Policy – Version 2.5

Effective Date: March 15, 2026

This Corporate Security Policy establishes the mandatory safeguards, controls, and operational expectations for all employees, contractors, and third-party service providers who interact with organizational systems, facilities, or data.

1. Purpose and Scope

This policy defines the comprehensive security requirements for safeguarding organizational digital assets, infrastructure, personnel, and physical facilities. It applies to employees, contractors, partners, and any entity accessing or processing company data.

The updated scope now includes cloud-native services, SaaS applications, CI/CD pipelines, and third-party integrations handling internal or customer data.

Business units must enforce these security standards consistently across all operational workflows.

This policy defines the comprehensive security requirements for safeguarding organizational digital assets, infrastructure, personnel, and physical facilities. It applies to employees, contractors, partners, and any entity accessing or processing company data.

The updated scope now includes cloud-native services, SaaS applications, CI/CD pipelines, and third-party integrations handling internal or customer data.

Business units must enforce these security standards consistently across all operational workflows.

This policy defines the comprehensive security requirements for safeguarding organizational digital assets, infrastructure, personnel, and physical facilities. It applies to employees, contractors, partners, and any entity accessing or processing company data.

The updated scope now includes cloud-native services, SaaS applications, CI/CD pipelines, and third-party integrations handling internal or customer data.

Business units must enforce these security standards consistently across all operational workflows.

This policy defines the comprehensive security requirements for safeguarding organizational digital assets, infrastructure, personnel, and physical facilities. It applies to employees, contractors, partners, and any entity accessing or processing company data.

The updated scope now includes cloud-native services, SaaS applications, CI/CD pipelines, and third-party integrations handling internal or customer data.

Business units must enforce these security standards consistently across all operational workflows.

2. Governance and Responsibilities

The CISO leads organizational security strategy, oversees compliance with ISO 27001 and SOC 2 controls, and coordinates quarterly reviews with Risk Management.

The Security Governance Committee meets monthly to evaluate risks, validate policies, and approve new security programs.

Business Unit Security Leads (BUSLs) are assigned to each department to enforce compliance and support audits.

All employees must complete quarterly security training and pass annual assessments.

The CISO leads organizational security strategy, oversees compliance with ISO 27001 and SOC 2 controls, and coordinates quarterly reviews with Risk Management.

The Security Governance Committee meets monthly to evaluate risks, validate policies, and approve new security programs.

Business Unit Security Leads (BUSLs) are assigned to each department to enforce compliance and support audits.

All employees must complete quarterly security training and pass annual assessments.

The CISO leads organizational security strategy, oversees compliance with ISO 27001 and SOC 2 controls, and coordinates quarterly reviews with Risk Management.

The Security Governance Committee meets monthly to evaluate risks, validate policies, and approve new security programs.

Business Unit Security Leads (BUSLs) are assigned to each department to enforce compliance and support audits.

All employees must complete quarterly security training and pass annual assessments.

The CISO leads organizational security strategy, oversees compliance with ISO 27001 and SOC 2 controls, and coordinates quarterly reviews with Risk Management.

The Security Governance Committee meets monthly to evaluate risks, validate policies, and approve new security programs.

Business Unit Security Leads (BUSLs) are assigned to each department to enforce compliance and support audits.

All employees must complete quarterly security training and pass annual assessments.

3. Access Control and Identity Management

All systems must enforce multi-factor authentication (MFA), including phishing-resistant options for administrators.

Privileged access follows RBAC and must be reviewed quarterly; automated provisioning is required.

Shared accounts are prohibited except for approved service accounts with full logging enabled.

Remote access requires zero-trust network access (ZTNA) with continuous risk-based evaluation.

Password standards include minimum 14 characters, complexity rules, and mandatory rotation every 60 days.

All systems must enforce multi-factor authentication (MFA), including phishing-resistant options for administrators.

Privileged access follows RBAC and must be reviewed quarterly; automated provisioning is required.

Shared accounts are prohibited except for approved service accounts with full logging enabled.

Remote access requires zero-trust network access (ZTNA) with continuous risk-based evaluation.

Password standards include minimum 14 characters, complexity rules, and mandatory rotation every 60 days.

All systems must enforce multi-factor authentication (MFA), including phishing-resistant options for administrators.

Privileged access follows RBAC and must be reviewed quarterly; automated provisioning is required.

Shared accounts are prohibited except for approved service accounts with full logging enabled.

Remote access requires zero-trust network access (ZTNA) with continuous risk-based evaluation.

Password standards include minimum 14 characters, complexity rules, and mandatory rotation every 60 days.

All systems must enforce multi-factor authentication (MFA), including phishing-resistant options for administrators.

Privileged access follows RBAC and must be reviewed quarterly; automated provisioning is required.

Shared accounts are prohibited except for approved service accounts with full logging enabled.

Remote access requires zero-trust network access (ZTNA) with continuous risk-based evaluation.

Password standards include minimum 14 characters, complexity rules, and mandatory rotation every 60 days.

4. Data Classification & Protection Requirements

Data classification includes: Public, Internal, Confidential, Restricted, and Regulated. Each tier has its own required controls per appendix.

Confidential/Restricted data must use AES-256 encryption at rest and TLS 1.3 in transit.

Backups must be encrypted, versioned, and retained for a minimum of 12 months with quarterly integrity checks.

Data retention schedules must be enforced, monitored, and reviewed annually by Compliance.

PII, PHI, and financial data must follow GDPR, HIPAA, PCI-DSS, and SOC 2 requirements.

Data classification includes: Public, Internal, Confidential, Restricted, and Regulated. Each tier has its own required controls per appendix.

Confidential/Restricted data must use AES-256 encryption at rest and TLS 1.3 in transit.

Backups must be encrypted, versioned, and retained for a minimum of 12 months with quarterly integrity checks.

Data retention schedules must be enforced, monitored, and reviewed annually by Compliance.

PII, PHI, and financial data must follow GDPR, HIPAA, PCI-DSS, and SOC 2 requirements.

Data classification includes: Public, Internal, Confidential, Restricted, and Regulated. Each tier has its own required controls per appendix.

Confidential/Restricted data must use AES-256 encryption at rest and TLS 1.3 in transit.

Backups must be encrypted, versioned, and retained for a minimum of 12 months with quarterly integrity checks.

Data retention schedules must be enforced, monitored, and reviewed annually by Compliance.

PII, PHI, and financial data must follow GDPR, HIPAA, PCI-DSS, and SOC 2 requirements.

Data classification includes: Public, Internal, Confidential, Restricted, and Regulated. Each tier has its own required controls per appendix.

Confidential/Restricted data must use AES-256 encryption at rest and TLS 1.3 in transit.

Backups must be encrypted, versioned, and retained for a minimum of 12 months with quarterly integrity checks.

Data retention schedules must be enforced, monitored, and reviewed annually by Compliance.

PII, PHI, and financial data must follow GDPR, HIPAA, PCI-DSS, and SOC 2 requirements.

5. Security Monitoring & Logging

All systems must forward logs to the centralized SIEM, with retention set to a minimum of 12 months.

Security alerts must follow standardized thresholds aligned with MITRE ATT&CK tactics.

Continuous monitoring must be enabled for cloud workloads, endpoints, and critical infrastructure.

Behavioral analytics and anomaly detection tools must be deployed across production systems.

All systems must forward logs to the centralized SIEM, with retention set to a minimum of 12 months.

Security alerts must follow standardized thresholds aligned with MITRE ATT&CK tactics.

Continuous monitoring must be enabled for cloud workloads, endpoints, and critical infrastructure.

Behavioral analytics and anomaly detection tools must be deployed across production systems.

All systems must forward logs to the centralized SIEM, with retention set to a minimum of 12 months.

Security alerts must follow standardized thresholds aligned with MITRE ATT&CK tactics.

Continuous monitoring must be enabled for cloud workloads, endpoints, and critical infrastructure.

Behavioral analytics and anomaly detection tools must be deployed across production systems.

All systems must forward logs to the centralized SIEM, with retention set to a minimum of 12 months.

Security alerts must follow standardized thresholds aligned with MITRE ATT&CK tactics.

Continuous monitoring must be enabled for cloud workloads, endpoints, and critical infrastructure.

Behavioral analytics and anomaly detection tools must be deployed across production systems.

6. Incident Response Procedures

All suspected incidents must be reported within 1 hour to the SOC through the incident portal.

Incident response follows NIST 800-61: Preparation → Detection → Analysis → Containment → Eradication → Recovery → Post-Incident Review.

Root cause analysis is required for all medium- and high-severity incidents and must be completed within 5 business days.

Incident findings must be documented and submitted to leadership quarterly, including trends and corrective actions.

All suspected incidents must be reported within 1 hour to the SOC through the incident portal.

Incident response follows NIST 800-61: Preparation → Detection → Analysis → Containment → Eradication → Recovery → Post-Incident Review.

Root cause analysis is required for all medium- and high-severity incidents and must be completed within 5 business days.

Incident findings must be documented and submitted to leadership quarterly, including trends and corrective actions.

All suspected incidents must be reported within 1 hour to the SOC through the incident portal.

Incident response follows NIST 800-61: Preparation → Detection → Analysis → Containment → Eradication → Recovery → Post-Incident Review.

Root cause analysis is required for all medium- and high-severity incidents and must be completed within 5 business days.

Incident findings must be documented and submitted to leadership quarterly, including trends and corrective actions.

All suspected incidents must be reported within 1 hour to the SOC through the incident portal.

Incident response follows NIST 800-61: Preparation → Detection → Analysis → Containment → Eradication → Recovery → Post-Incident Review.

Root cause analysis is required for all medium- and high-severity incidents and must be completed within 5 business days.

Incident findings must be documented and submitted to leadership quarterly, including trends and corrective actions.

Appendix B: Regulatory References

Mapping of controls to: GDPR Articles 5, 25, 32; ISO 27001 Annex A; SOC 2 Security & Availability criteria; HIPAA §164.

Definitions of regulatory terms including Data Controller, Data Processor, Lawful Basis, and DPIA requirements.

Crosswalk tables comparing Version 1.0 to Version 2.5 for audit readiness.

Mapping of controls to: GDPR Articles 5, 25, 32; ISO 27001 Annex A; SOC 2 Security & Availability criteria; HIPAA §164.

Definitions of regulatory terms including Data Controller, Data Processor, Lawful Basis, and DPIA requirements.

Crosswalk tables comparing Version 1.0 to Version 2.5 for audit readiness.

Mapping of controls to: GDPR Articles 5, 25, 32; ISO 27001 Annex A; SOC 2 Security & Availability criteria; HIPAA §164.

Definitions of regulatory terms including Data Controller, Data Processor, Lawful Basis, and DPIA requirements.

Crosswalk tables comparing Version 1.0 to Version 2.5 for audit readiness.