Corporate Security Policy – Version 1.0

Effective Date: January 1, 2024

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 minimum security requirements for protecting organizational systems, data, employees, and physical assets. It applies to all full-time employees, part-time workers, interns, contractors, and vendors with access to company resources.

The scope includes corporate networks, cloud environments, end-user devices, on-premises infrastructure, and any workflow that involves the processing or transmission of company data.

This policy defines the minimum security requirements for protecting organizational systems, data, employees, and physical assets. It applies to all full-time employees, part-time workers, interns, contractors, and vendors with access to company resources.

The scope includes corporate networks, cloud environments, end-user devices, on-premises infrastructure, and any workflow that involves the processing or transmission of company data.

This policy defines the minimum security requirements for protecting organizational systems, data, employees, and physical assets. It applies to all full-time employees, part-time workers, interns, contractors, and vendors with access to company resources.

The scope includes corporate networks, cloud environments, end-user devices, on-premises infrastructure, and any workflow that involves the processing or transmission of company data.

This policy defines the minimum security requirements for protecting organizational systems, data, employees, and physical assets. It applies to all full-time employees, part-time workers, interns, contractors, and vendors with access to company resources.

The scope includes corporate networks, cloud environments, end-user devices, on-premises infrastructure, and any workflow that involves the processing or transmission of company data.

2. Governance and Responsibilities

The Chief Information Security Officer (CISO) oversees policy implementation, annual reviews, and reports to executive leadership on security posture.

Department managers are responsible for ensuring that staff follow security controls relevant to their business functions.

The Security Operations Team manages monitoring, incident triage, vulnerability scanning, and control verification activities on a recurring basis.

Employees must adhere to mandatory security training and immediately report suspicious activity.

The Chief Information Security Officer (CISO) oversees policy implementation, annual reviews, and reports to executive leadership on security posture.

Department managers are responsible for ensuring that staff follow security controls relevant to their business functions.

The Security Operations Team manages monitoring, incident triage, vulnerability scanning, and control verification activities on a recurring basis.

Employees must adhere to mandatory security training and immediately report suspicious activity.

The Chief Information Security Officer (CISO) oversees policy implementation, annual reviews, and reports to executive leadership on security posture.

Department managers are responsible for ensuring that staff follow security controls relevant to their business functions.

The Security Operations Team manages monitoring, incident triage, vulnerability scanning, and control verification activities on a recurring basis.

Employees must adhere to mandatory security training and immediately report suspicious activity.

The Chief Information Security Officer (CISO) oversees policy implementation, annual reviews, and reports to executive leadership on security posture.

Department managers are responsible for ensuring that staff follow security controls relevant to their business functions.

The Security Operations Team manages monitoring, incident triage, vulnerability scanning, and control verification activities on a recurring basis.

Employees must adhere to mandatory security training and immediately report suspicious activity.

3. Access Control and Identity Management

User accounts are provisioned upon hiring and require approval from the hiring manager and IT.

Password-only authentication is permitted as long as passwords are 10+ characters and rotated every 120 days.

Privileged accounts are assigned manually and reviewed annually.

Remote access requires VPN use but does not mandate MFA for all roles.

Shared accounts may be used in limited operational contexts with manager approval.

User accounts are provisioned upon hiring and require approval from the hiring manager and IT.

Password-only authentication is permitted as long as passwords are 10+ characters and rotated every 120 days.

Privileged accounts are assigned manually and reviewed annually.

Remote access requires VPN use but does not mandate MFA for all roles.

Shared accounts may be used in limited operational contexts with manager approval.

User accounts are provisioned upon hiring and require approval from the hiring manager and IT.

Password-only authentication is permitted as long as passwords are 10+ characters and rotated every 120 days.

Privileged accounts are assigned manually and reviewed annually.

Remote access requires VPN use but does not mandate MFA for all roles.

Shared accounts may be used in limited operational contexts with manager approval.

User accounts are provisioned upon hiring and require approval from the hiring manager and IT.

Password-only authentication is permitted as long as passwords are 10+ characters and rotated every 120 days.

Privileged accounts are assigned manually and reviewed annually.

Remote access requires VPN use but does not mandate MFA for all roles.

Shared accounts may be used in limited operational contexts with manager approval.

4. Data Classification & Protection Requirements

Data is classified into Public, Internal, Confidential, and Restricted categories. Handling expectations vary based on classification level.

Confidential and Restricted data must use encryption where feasible but exceptions may be approved by IT leadership.

Backups are performed weekly and retained for 90 days across cloud and on-prem systems.

Data retention schedules are recommended but not enforced across all departments.

Data is classified into Public, Internal, Confidential, and Restricted categories. Handling expectations vary based on classification level.

Confidential and Restricted data must use encryption where feasible but exceptions may be approved by IT leadership.

Backups are performed weekly and retained for 90 days across cloud and on-prem systems.

Data retention schedules are recommended but not enforced across all departments.

Data is classified into Public, Internal, Confidential, and Restricted categories. Handling expectations vary based on classification level.

Confidential and Restricted data must use encryption where feasible but exceptions may be approved by IT leadership.

Backups are performed weekly and retained for 90 days across cloud and on-prem systems.

Data retention schedules are recommended but not enforced across all departments.

Data is classified into Public, Internal, Confidential, and Restricted categories. Handling expectations vary based on classification level.

Confidential and Restricted data must use encryption where feasible but exceptions may be approved by IT leadership.

Backups are performed weekly and retained for 90 days across cloud and on-prem systems.

Data retention schedules are recommended but not enforced across all departments.

5. Security Monitoring & Logging

Security logs are collected from core infrastructure and reviewed on a best-effort basis by IT.

Only critical systems are integrated into centralized log storage.

Alert thresholds are adjusted by system owners but not standardized organization-wide.

Log data is retained for at least 30 days unless storage issues arise.

Security logs are collected from core infrastructure and reviewed on a best-effort basis by IT.

Only critical systems are integrated into centralized log storage.

Alert thresholds are adjusted by system owners but not standardized organization-wide.

Log data is retained for at least 30 days unless storage issues arise.

Security logs are collected from core infrastructure and reviewed on a best-effort basis by IT.

Only critical systems are integrated into centralized log storage.

Alert thresholds are adjusted by system owners but not standardized organization-wide.

Log data is retained for at least 30 days unless storage issues arise.

Security logs are collected from core infrastructure and reviewed on a best-effort basis by IT.

Only critical systems are integrated into centralized log storage.

Alert thresholds are adjusted by system owners but not standardized organization-wide.

Log data is retained for at least 30 days unless storage issues arise.

6. Incident Response Procedures

Incidents must be reported within 24 hours to the IT helpdesk or security@company.com.

Incident phases follow: Detection, Containment, Recovery, and Post-Event Review.

Root cause analysis is performed for major incidents only.

Incident records are stored for six months, with optional quarterly reporting to leadership.

Incidents must be reported within 24 hours to the IT helpdesk or security@company.com.

Incident phases follow: Detection, Containment, Recovery, and Post-Event Review.

Root cause analysis is performed for major incidents only.

Incident records are stored for six months, with optional quarterly reporting to leadership.

Incidents must be reported within 24 hours to the IT helpdesk or security@company.com.

Incident phases follow: Detection, Containment, Recovery, and Post-Event Review.

Root cause analysis is performed for major incidents only.

Incident records are stored for six months, with optional quarterly reporting to leadership.

Incidents must be reported within 24 hours to the IT helpdesk or security@company.com.

Incident phases follow: Detection, Containment, Recovery, and Post-Event Review.

Root cause analysis is performed for major incidents only.

Incident records are stored for six months, with optional quarterly reporting to leadership.

Appendix A: Definitions

Sensitive Data: Any data that could cause organizational, financial, or reputational harm if disclosed.

Critical System: Any system supporting revenue operations, core infrastructure, or regulated workflows.

User Credentials: Passwords, tokens, or other identifiers used for system authentication.

Sensitive Data: Any data that could cause organizational, financial, or reputational harm if disclosed.

Critical System: Any system supporting revenue operations, core infrastructure, or regulated workflows.

User Credentials: Passwords, tokens, or other identifiers used for system authentication.

Sensitive Data: Any data that could cause organizational, financial, or reputational harm if disclosed.

Critical System: Any system supporting revenue operations, core infrastructure, or regulated workflows.

User Credentials: Passwords, tokens, or other identifiers used for system authentication.