Nova Company- IT Policy
Version: 1.0
Effective Date: 22-10-2025
Review Date: 31-12-2025
Document Owner: Chief Information Officer (CIO)
Approved by: [Executive Sponsor / Board]
Table of Contents

28. Purpose and Nature of the IT Policy
This IT Policy establishes the principles, minimum requirements and governance necessary to ensure the secure, reliable, cost-effective and compliant use of information technology across [Company Name]. It defines responsibilities, processes and controls that support business objectives while protecting corporate information assets, customers, employees and partners from operational, legal and reputational risk.

This policy is strategic in nature and sets mandatory baseline requirements. Operational procedures, standards, guidelines and work instructions that implement the policy are maintained separately and linked as references.

1. Applicability and Scope

2.1 Applicability

This policy applies to:

- All employees, contractors, consultants, temporaries and other workers at [Company Name] (collectively “Users”).
- All IT systems, applications, platforms, networks and services owned, provisioned, leased or used by [Company Name].
- All information assets created, processed, transmitted or stored on corporate systems, including data held by third-party processors.
- All physical locations and facilities where company IT assets are stored or operate.

2.2 Exclusions

Any exception to this policy must be formally approved through the Dispensation (Exception) Process described in section 3.4.

1. Document Structure, Storage and Control

3.1 Document Structure

This policy is the top-level IT governance document. It is supported by related documents:

- Standards: Mandatory technical specifications (e.g., encryption standard, password standard).
- Procedures: Step-by-step operational instructions to implement standards (e.g., user provisioning procedure).
- Guidelines: Recommended best practices.
- Templates and Forms: For change requests, incident reports, SLA templates, etc.

3.2 Document Storage & Control

- The official version of this policy and supporting documents shall be stored in the Document Management System (DMS) designated by IT Governance (e.g., SharePoint, Confluence).
- Documents shall be version-controlled, access-restricted by role, and archived according to Records Retention schedules.
- The Document Owner (CIO) is responsible for ensuring documents are current and accessible to authorized personnel.

3.3 Change Control

- Changes to this policy follow a formal review and approval workflow: Draft → Review (stakeholders) → Legal/Compliance review → Executive approval → Publication.
- A change log will be maintained listing version number, author, summary of changes, effective date.
- Significant changes require communication to all affected Users and training as necessary.

3.4 Dispensation (Exception) Process

- Exceptions may be requested via the Exception Request form (Appendix C).
- Requests must include business justification, risk assessment, compensating controls, and expiry date.
- The Exception Review Board (ERB), comprising IT Governance, Security Officer, Legal/Compliance, and relevant business owners, will review and approve/deny exceptions.
- Approved exceptions are time-limited and subject to periodic review.

1. IT Organization and Roles & Responsibilities

4.1 IT Organizational Principles

- IT operates as an enabling business function governed by the CIO with clear separation between governance, architecture, operations, security, and development responsibilities.

- Clear lines of accountability, documented role descriptions, and segregation of duties (SoD) shall be maintained.

4.2 Core Roles and Responsibilities (high-level)

- Executive Sponsor: Endorses and funds IT strategy.
- CIO (Document Owner): Overall responsibility for IT policy, strategy and delivery.
- IT Governance Committee: Oversees IT risk, policy, strategy and major investments.
- IT Security Officer / CISO: Responsible for information security program, policies and incident response.
- IT Operations Manager: Responsible for day-to-day run of production environments.
- Application Owners / System Owners: Accountable for security, availability and compliance of specific systems.
- Data Owners/Stewards: Accountable for data classification, quality and access decisions.
- Service Desk: First-line support and incident triage.
- Users: Comply with policies and report incidents.

(See Appendix B for detailed role matrix.)

1. IT Strategy and Planning

5.1 Policy Statements

- IT will align with corporate strategy and support business goals via a documented IT Strategy updated at least annually.
- The IT Strategy will include capability roadmaps, architecture principles, cloud strategy, data management strategy, security roadmap and prioritized initiatives.
- Technology investments will be informed by business value, risk, total cost of ownership (TCO), and compliance requirements.

5.2 Planning Processes

- Annual planning cycle: business requirements gathering, prioritization, budget submission, and architecture review.
- All major projects must demonstrate alignment to IT Strategy and receive approval via the IT Governance Committee.

1. IT Cost Management and Procurement

6.1 Budgeting and Cost Control

- IT budgets (capital and operating) are managed centrally and require justification, ROI analysis and executive approval.
- Cost allocation or charge-back models should be transparent where applicable.

6.2 Procurement and Vendor Onboarding

- All IT procurements follow centralized procurement processes that include security, privacy and legal assessments.
- Standard procurement contracts must include data protection, service levels, right-to-audit, termination and transition clauses.

1. Management Reporting of IT Performance

7.1 KPIs and Metrics

- IT performance will be monitored via KPIs, including system availability, incident resolution times, mean time to restore (MTTR), percentage of critical patches applied, SLA compliance, project delivery metrics and security metrics (e.g., vulnerabilities, incidents).
- Reports are produced for different audiences: operational dashboards for IT management, monthly reports for Executive Team, quarterly reports for Board.

7.2 Frequency and Distribution

- Daily operational dashboards for NOC and Ops.
- Weekly summaries for IT leadership.
- Monthly reports to business stakeholders.

- Quarterly executive and Board-level IT performance and risk reports.

1. Service Level Management

8.1 SLAs and OLAs

- Service Level Agreements (SLAs) shall be defined for critical services and agreed with business owners.
- Operational Level Agreements (OLAs) define internal support responsibilities.
- SLAs must include availability, response times, escalation procedures and performance measurement.

8.2 Monitoring and Reviews

- Service performance will be monitored and SLA compliance reviewed monthly.
- Incidents resulting in SLA breaches require root cause analysis and corrective action plans.

1. Legal and Regulatory Compliance

9.1 Policy Statements

- IT must comply with applicable laws, regulations and contractual obligations (e.g., data protection laws such as GDPR, industry standards like PCI-DSS, HIPAA where applicable).
- Legal and Compliance must be engaged early in projects that involve personal data, regulated data or cross-border data flows.

9.2 Data Protection and Privacy

- Data classification must be used to determine handling requirements (e.g., Public, Internal, Confidential, Restricted).
- Personal Identifiable Information (PII) must be processed only where necessary, protected by appropriate controls, and handled per privacy notices and DPAs.

9.3 Record Keeping and eDiscovery

- IT must implement retention schedules and support legal holds as required by Legal.

1. IT Asset Management

10.1 Asset Inventory and Ownership

- All IT assets (hardware, software, cloud instances, virtual assets, licenses) must be inventoried and assigned to an Asset Owner.
- The inventory must be maintained in the Asset Management System and reconciled quarterly.

10.2 Software Licensing and Compliance

- Software must be legally procured and usage tracked against licenses.
- Unauthorized software is prohibited; audit and remediation plans are required for non-compliance.

10.3 Asset Lifecycle

- Policies must cover acquisition, deployment, maintenance, secure disposal and data sanitization procedures for end-of-life equipment.

1. Managing Third-Party Services

11.1 Due Diligence and Risk Assessment

- Third parties providing IT services are subject to risk-based due diligence (security posture, financial stability, reputation).
- High-risk vendors require on-site assessment, questionnaires and security testing.

11.2 Contracts and Data Protection

- Contracts must include SLAs, data protection clauses, confidentiality, incident notification requirements, subprocessor restrictions, and right-to-audit.

11.3 Ongoing Vendor Management

- Regular performance and security reviews; access by third parties is restricted and monitored.
- Termination and transition plans must be included to ensure continuity.

1. Operations Management

12.1 Monitoring and Event Management

- Production environments must be monitored 24/7 (where critical) for availability, performance and security alerts.
- Events are logged and triaged per incident response processes.

12.2 Scheduled Maintenance

- Maintenance windows are approved, communicated in advance, and implemented with rollback plans and testing.

12.3 Backup and Restore

- Backup strategy must support required RTO/RPO for critical systems.
- Backups must be encrypted, periodically tested for integrity and stored in geographically separated locations where appropriate.

12.4 Job Scheduling and Batch Operations

- Job schedules must be documented; failures are alerted and handled per runbook procedures.

1. Development Methodology and Secure SDLC

13.1 Development Principles

- Development follows a documented methodology (e.g., Agile/Scrum, DevOps) with segregation between development, test and production environments.
- Infrastructure-as-Code and automated pipelines are encouraged with controls.

13.2 Secure SDLC Requirements

- Security requirements, threat modeling, secure coding standards, static/dynamic analysis, vulnerability scanning and penetration testing must be integrated into the lifecycle.
- Code reviews, environment segregation, test data masking, and pre-release security acceptance criteria are mandatory for production deployments.

13.3 Version Control, Release Management and Configuration Management

- Source code must be in authorized version control systems.
- Release artifacts must be traceable and managed via approved release processes.

1. Change Management

14.1 Change Control Process

- All changes to production systems require a Change Request (CR), risk assessment and approval from the Change Advisory Board (CAB) except emergency changes processed via the Emergency Change Procedure.
- Change windows, rollback plans, communication and post-implementation review are required.

14.2 Emergency Changes

- Emergency changes must be documented, time-limited, reviewed after implementation and subject to retrospective CAB approval.

14.3 Change Classification

- Changes are classified (standard, minor, major, emergency) with corresponding approval levels and testing requirements.

1. Logical Access Controls (Identity & Access Management)

15.1 Account Management

- Accounts are issued based on need and approved access requests; principle of least privilege applies.
- User provisioning/termination must be integrated with HR processes for timely updates.

15.2 Authentication and Passwords

- Multi-Factor Authentication (MFA) is required for access to sensitive systems, remote access, privileged accounts and administrative interfaces.
- Password policy enforces strength, expiration, reuse and storage requirements consistent with industry best practices.

15.3 Authorization and Role-Based Access

- Access is role-based where possible; separation of duties must prevent conflicting privileges.

- Periodic access reviews (at least quarterly for privileged accounts, semi-annually for other accounts) are mandatory.

15.4 Privileged Access Management (PAM)

- Administrative and privileged access must be controlled via PAM solutions, session recording, and just-in-time access workflows.

15.5 Remote Access and VPN

- Remote access must use secure VPN or SASE solutions and enforce device security posture checks.

1. Physical Access Controls

16.1 Facilities and Data Centers

- Data centers and critical IT facilities must have controlled physical access (badging, biometrics, visitor logs), CCTV, environmental controls and fire suppression.
- Access to server rooms is restricted to authorized personnel and logged.

16.2 Office Security and Mobile Devices

- Laptops and mobile devices must be secured when unattended. Visitors must be escorted and sign visitor logs.

16.3 Asset Labeling and Storage

- Assets are tagged and storage locations tracked. Secure storage for backup media and removable devices is required.

1. Computer Operations

17.1 Logging and Monitoring

- System and application logs must be retained per retention schedules and protected against tampering.
- Centralized logging with SIEM for security-critical systems is required.

17.2 Patch Management

- Critical and security patches must be applied within defined SLAs based on severity; patch testing is required for production systems.
- Unpatched systems represent an elevated risk and must have compensating controls where immediate patching is not feasible.

17.3 Change and Release Controls

- Operations teams must coordinate closely with development to ensure releases follow agreed processes and approvals.

1. Network Security

18.1 Architecture and Segmentation

- Network architecture must enforce segmentation between production, development, DMZ, and guest networks to reduce attack surface.
- Firewalls, network access control (NAC), and micro-segmentation where appropriate.

18.2 Perimeter and Ingress Controls

- External facing services must be hardened, patched, and subject to regular vulnerability scans and penetration testing.
- Web application firewalls (WAF), DDoS protection and rate limiting should be implemented where needed.

18.3 Wireless and Remote Access

- Corporate Wi-Fi must be secured with enterprise encryption and periodic credential rotation; guest Wi-Fi must be isolated from corporate resources.

18.4 Network Monitoring and Threat Detection

- Network traffic is monitored for anomalies; IDS/IPS and threat detection capabilities applied as appropriate.

1. End-User Computing (Workstations, Mobile Devices, BYOD)

19.1 Device Standardization and Configuration

- Minimal supported device configurations and hardened images shall be defined and used.
- Host-based security (antivirus/EDR), disk encryption and endpoint management are mandatory.

19.2 Software Installation and Use

- Users may only use approved and licensed software. Installation rights are restricted to authorized IT personnel.

19.3 BYOD and Mobile Device Policy

- BYOD is permitted only under a registered program with MDM/EMM, data segregation, and accepted terms including remote wipe capabilities.
- Sensitive corporate data is prohibited on unmanaged devices.

19.4 Removable Media

- Use of removable media (USB drives) is restricted; scanned and encrypted devices only with documented business justification.

1. E-mail Policy

20.1 Acceptable Use

- Corporate e-mail is for business use. Personal use must be limited and not interfere with duties.

20.2 Confidentiality and Encryption

- Confidential or sensitive information transmitted via email requires encryption (TLS in transit and, for sensitive content, end-to-end or file-level encryption).
- Sensitive attachments should be password-protected and shared via secure file transfer where appropriate.

20.3 Phishing and Fraud Awareness

- Users must be trained to recognize and report phishing. Suspicious messages must be reported to IT Security immediately.

20.4 Retention and Archiving

- E-mail retention follows Records Management policies and regulatory requirements. Archiving and eDiscovery processes must be supported.

1. Virus and Malicious Code Security Policy

21.1 Endpoint Protection

- All endpoints and servers must have centrally-managed anti-malware/EDR solutions with automatic updates and real-time protection.

21.2 Scanning and Updates

- Regular scans, signature and behavioral updates must be enforced. Suspicious files are quarantined and analyzed.

21.3 Incident Response and Containment

- Malware incidents are treated per the Incident Response Plan: isolation, eradication, recovery and root cause analysis.

21.4 User Education

- Regular malicious code awareness training and simulated phishing campaigns will be executed.

1. Business Continuity and Disaster Recovery Planning

22.1 BCP/DR Policy Statements

- Business Continuity Plans (BCP) and Disaster Recovery (DR) Plans must exist for critical services, with defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Critical processes identified through Business Impact Analysis (BIA) will be prioritized for recovery planning.

22.2 Backup, Redundancy and Failover

- Disaster recovery strategies include backups, standby systems, geographic redundancy, and documented recovery procedures.

22.3 Testing and Exercises

- BCP/DR plans will be tested annually or more frequently as required. Test results and gap remediation are documented.

22.4 Crisis Communication

- A communication plan for internal and external stakeholders during incidents must be maintained, including notification templates.

1. Compliance and Audit

23.1 Internal and External Audit

- IT will support periodic internal and external audits of controls, compliance frameworks and regulatory requirements.
- Audit findings must be tracked, remediated, and reported until closed.

23.2 Continuous Compliance Monitoring

- Automated controls and monitoring will be used where feasible to provide continuous assurance over compliance posture.

23.3 Evidence and Records

- IT must maintain and provide evidence as required for compliance (logs, change records, configuration snapshots).

1. Website Policy

24.1 Content and Change Control

- Public-facing website content must be approved and updated through controlled processes. Content owners are accountable for accuracy and appropriateness.

24.2 Security and Hosting

- Websites must use HTTPS with strong TLS configuration, regular vulnerability scanning, WAF protection and secure coding practices.
- Administrative interfaces must be protected by MFA and limited access.

24.3 Privacy and Cookies

- Websites must present clear privacy notices and cookie policies consistent with applicable laws and collect consent where required.

24.4 Monitoring and Incident Response

- Websites are monitored for performance, uptime and defacement. Incident response for web compromises follows standard IR procedures.

1. Training, Awareness and Competency

- Role-based security and IT awareness training is mandatory for all Users upon hire and annually thereafter.
- Specialized training for IT, developers, privileged users and incident responders must be provided and tracked.

1. Policy Enforcement and Sanctions

- Non-compliance with this policy may result in disciplinary action up to and including termination, and, where appropriate, legal action.
- Security incidents caused by willful negligence or policy violations will be escalated to HR and Legal.

1. Review and Maintenance of this Policy

- This policy will be reviewed at least annually or after material changes to the business, technology landscape, legal/regulatory environment, or after major incidents.
- The Document Owner is responsible for initiating reviews and obtaining approvals.

Appendix A — Definitions and Acronyms (selected)

- Asset Owner: Individual responsible for the management and use of an IT asset.
- CAB: Change Advisory Board.
- CIO: Chief Information Officer.
- CISO: Chief Information Security Officer.

- DPA: Data Processing Agreement.
- DR: Disaster Recovery.
- EDR: Endpoint Detection and Response.
- ERB: Exception Review Board.
- HR: Human Resources.
- IT: Information Technology.
- KPI: Key Performance Indicator.
- MFA: Multi-Factor Authentication.
- NOC: Network Operations Center.
- PAM: Privileged Access Management.
- PCI-DSS: Payment Card Industry Data Security Standard.
- PII: Personally Identifiable Information.
- RPO: Recovery Point Objective.
- RTO: Recovery Time Objective.
- SIEM: Security Information and Event Management.
- SLA: Service Level Agreement.

Appendix B — Roles and Responsibility Matrix (summary)

- Executive Sponsor: Strategic oversight and funding.
- CIO: Policy owner and strategic alignment.
- IT Governance Committee: Approvals and risk oversight.
- CISO/IT Security: Security policy enforcement, incident response.
- IT Operations: Runbook execution, monitoring, maintenance.
- Application/System Owners: Day-to-day operations, change approval for their systems.
- Data Owners: Classification and access decisions.
- Procurement/Legal: Vendor contracts and compliance.
- HR: Onboarding/offboarding and disciplinary actions.

(Full matrix available in the DMS.)

Appendix C — Templates (samples)

- Change Request Template: Summary, Impact, Risk Assessment, Rollback Plan, Test Plan, Proposed Window, Approvals.
- Exception Request Template: Business Justification, Technical Details, Risk Assessment, Compensating Controls, Expiry Date, Approvers.

Appendix D — Reference Standards and Related Policies

- Related documents include: Information Security Policy, Acceptable Use Policy, Data Classification Standard, Password Standard, Backup & Retention Procedure, Incident Response Plan, Vendor Management Standard, Privacy Policy, Business Continuity Plan.
- External frameworks: ISO/IEC 27001, NIST SP 800-53/800-171, GDPR, PCI-DSS where applicable.