NovaTech Dynamics Information Security Policy

Document Control Information

- **Document Owner**: Sarah Chen, Chief Information Security Officer
- **Document ID**: NTD-SEC-001-2025
- **Version**: 3.2
- **Last Updated**: January 15, 2025
- **Approved By**: Michael Rodriguez, CEO
- **Effective Date**: February 1, 2025

Definition of Security

Information security in NovaTech Dynamics' IT systems is understood as ensuring:

- **Confidentiality** of information (preventing access to data by third parties)
- **Integrity** of information (avoiding unauthorized changes to data)
- **Availability** of information (ensuring access to data at any time required by the user)
- **Accountability** of operations performed on information (ensuring that complete access history is stored with information about who obtained such access)

NovaTech Dynamics' Management Board applies adequate measures to ensure information security across all company operations at our headquarters (87 Innovation Drive, Boston, MA) and regional offices.

Data Classification System

NovaTech Dynamics employs a three-tier data classification system:

1. **Level 1 - Restricted**: Highest sensitivity (e.g., proprietary algorithms, financial forecasts)
2. **Level 2 - Confidential**: Medium sensitivity (e.g., customer data, employee records)
3. **Level 3 - Internal**: Low sensitivity (e.g., general communications, non-sensitive documentation)

The following are considered data subject to special protection (Level 1 & 2):

- Information about contracts being implemented with key clients including Westfield Healthcare, GlobalTech, and Federal agencies
- Financial information including quarterly revenue figures, profit margins, and investment strategies
- Organizational information including restructuring plans, mergers and acquisition strategies
- Access data to NovaTech Azure cloud environment, Oracle database systems, and internal networks

- Personal data of employees, contractors, and clients as defined in our GDPR and CCPA compliance documentation
- Research & Development information constituting the Company's competitive advantage including AI model parameters and proprietary algorithms
- Other information explicitly marked as "confidential information" or "restricted data"

Principle of Minimal Privileges

When granting access rights to data processed in NovaTech Dynamics' IT systems, the "minimal privileges" principle must be applied, meaning assigning the minimum privileges necessary to perform work at a given position.

Example: Development team members have read-access to the code repository for their specific project, but only designated team leads have write privileges. System administrators in the IT Operations Department have administrator access to their assigned systems only, not enterprise-wide privileges.

Principle of Multi-layer Security

NovaTech Dynamics implements security in depth with multiple defensive layers:

1. **Network Security**: Cisco Next-Gen firewalls, network segmentation, intrusion detection
2. **Endpoint Security**: Carbon Black EDR solution, Windows Defender, regular vulnerability scanning
3. **Application Security**: OWASP standards implementation, regular code security reviews
4. **Data Security**: Encryption, access controls, data loss prevention
5. **Physical Security**: Badge access, biometric verification for server rooms

Example: Our customer database (Oracle CRM system) is protected by network-level firewall rules, application-level authentication, data encryption at rest and in transit, and regular security audits conducted by our Security Operations Center team.

Principle of Access Restriction

The default permissions in NovaTech Dynamics' IT systems follow a "deny by default" approach:

- New employees receive access only to basic systems (email, intranet, time tracking)
- Additional access requires managerial approval via our ServiceNow ticketing system
- Privileged access (e.g., production environments) requires CISO and department head approval
- Temporary access expires automatically after the approved timeframe

Example: When the Marketing Department requires access to customer demographic data for campaign analysis, the request must be approved by both the Marketing Director and Data Protection Officer before Database Administrators grant time-limited access.

Access to Confidential Data on PC Workstations

- Access to confidential data in the NovaTech Dynamics LAN is implemented on dedicated secure servers (srvprod01, srvprod02, and srvdata01) located in the secure server room on Floor 3
- All access attempts to confidential data (successful or unsuccessful) are logged in our Splunk SIEM system with automated alerts for suspicious activities
- All company laptops utilize BitLocker encryption with TPM verification and secure boot
- Remote access to confidential data requires VPN with multi-factor authentication using our Okta identity management system
- Access to confidential data through the company WiFi network requires 802.1X authentication and encrypted VPN tunnel using Cisco AnyConnect

Workstation Security Requirements

NovaTech Dynamics workstations must adhere to the following security baseline:

- CrowdStrike Falcon EDR platform and Microsoft Defender for Endpoint with real-time protection
- Automatic Windows updates managed through WSUS server with forced monthly patching cycle
- Complex password requirements enforced via Active Directory Group Policy (details in section VII)
- Automatic screen lock after 10 minutes of inactivity
- Standard user accounts for daily operations; admin access via PAM solution for authorized staff only

Password Policy

- Passwords must be changed every 90 days through our automated password management system
- Password history of 12 previous passwords is maintained to prevent reuse
- All passwords must be stored in encrypted format using industry-standard hashing algorithms (SHA-256 minimum)
- Password requirements:
    - Minimum 12 characters
    - At least one uppercase letter
    - At least one lowercase letter
    - At least one number
    - At least one special character
    - No dictionary words or common patterns
- All system administrators and employees with access to Level 1 data must use the company-provided LastPass Enterprise password manager

Employee Responsibility for Confidential Data

Each NovaTech Dynamics employee signs a Confidentiality Agreement as part of their onboarding process and is responsible for maintaining the confidentiality of data they access. Violations may result in disciplinary action as outlined in the Employee Handbook, Section 8.3.

Security Monitoring Program

NovaTech Dynamics' Security Operations Center (SOC) monitors the following:

- Network traffic analysis using Darktrace AI security platform
- Endpoint behavioral analysis via CrowdStrike Falcon EDR
- Authentication logs across all systems via Splunk SIEM
- Cloud infrastructure monitoring via Microsoft Cloud App Security
- Data access and movement patterns via Varonis DatAdvantage
- Web filtering logs from Zscaler proxy services

Security monitoring is conducted in compliance with all applicable laws including employee privacy regulations, with annual legal review of monitoring practices.

Security Awareness Program

NovaTech Dynamics implements a comprehensive security training program:

- All new employees complete mandatory security awareness training within first 30 days
- Quarterly security refresher courses delivered via our Cornerstone LMS platform
- Monthly phishing simulation exercises with targeted training for employees who fail tests
- Role-specific advanced security training for IT, Development, and Finance teams
- Annual compliance training on GDPR, HIPAA, and industry-specific regulations

Approved Technologies and Tools

NovaTech Dynamics maintains an approved technology list. Only software and services on this list may be used for company purposes:

- **Productivity**: Microsoft 365 Suite, Adobe Creative Cloud
- **Development**: GitHub Enterprise, Visual Studio, GitLab
- **Communication**: Microsoft Teams, Zoom (Enterprise account only)
- **Storage**: OneDrive for Business, SharePoint, Azure Blob Storage
- **Mobile**: Company-provided devices with MDM enrollment only

Mobile Device Management

All mobile devices accessing NovaTech Dynamics data must:

- Be enrolled in Microsoft Intune MDM solution
- Have company security profile installed

- Enable full-disk encryption
- Use biometric or 6+ digit passcode

Incident Response Protocol

Security incidents must be reported immediately to the Security Operations Center:

- Email: soc@novatechdynamics.com
- Phone: Internal extension 4911
- Teams: @Security Response Team

The Incident Response Team follows the documented IR playbooks based on incident type, with response times of:

- Critical: 15 minutes
- High: 1 hour
- Medium: 4 hours
- Low: 24 hours

Backup and Recovery

- Critical systems (ERP, CRM, financial systems) are backed up hourly to secure storage
- All production databases are backed up daily with transaction log shipping
- Backup media is encrypted using AES-256 encryption
- Offsite backups are stored at Iron Mountain secure facility with quarterly pickup
- Recovery testing is performed monthly on randomly selected systems
- Full disaster recovery test is conducted bi-annually

Employee Termination Process

When employment is terminated:

1. HR initiates offboarding workflow in ServiceNow
2. All access is revoked within 4 hours of termination notification
3. Equipment is collected and sanitized according to NIST standards
4. Digital access cards are deactivated
5. Password resets are forced on shared systems

Annual Security Assessment

NovaTech Dynamics conducts the following security assessments:

- Quarterly vulnerability scanning of all systems
- Annual penetration testing by external security firm (currently Mandiant)
- Bi-annual security policy review
- Annual compliance audit (SOC 2 Type II)

Compliance Framework

This security policy helps NovaTech Dynamics maintain compliance with:

- ISO 27001
- SOC 2 Type II
- GDPR
- HIPAA (for healthcare client data)
- NIST Cybersecurity Framework

Policy Acknowledgement

All employees must acknowledge receipt and understanding of this policy during onboarding and after any major revisions. Current acknowledgement rate: 97% of employees (as of January 2025).

Contact Information

For questions regarding this policy, contact:

- Information Security Team: security@novatechdynamics.com
- IT Helpdesk: helpdesk@novatechdynamics.com / ext. 2000
- Data Protection Officer: dpo@novatechdynamics.com / ext. 3045