NovaTech Solutions — Information Security Policy

Document ID: NT-ISP-2025-003 **Version:** 3.2 **Effective Date:** January 15, 2025
Last Reviewed: January 10, 2025 **Next Review Date:** July 15, 2025
Classification: Internal **Owner:** Chief Information Security Officer (CISO)
Approved By: Executive Leadership Team

---

1. Purpose and Scope

1.1 Purpose

This Information Security Policy establishes the security requirements, standards, and procedures that govern the protection of information assets at NovaTech Solutions ("NovaTech," "the Company"). The policy exists to safeguard the confidentiality, integrity, and availability of all data entrusted to NovaTech by its customers, partners, employees, and other stakeholders.

1.2 Scope

This policy applies to all NovaTech employees, contractors, temporary staff, interns, and third-party service providers who access, process, store, or transmit NovaTech information assets. It covers all information systems, networks, applications, and data repositories operated by or on behalf of NovaTech, including cloud-hosted infrastructure, on-premises systems, and employee endpoints.

1.3 Policy Authority

The Chief Information Security Officer (CISO) is the designated authority for the interpretation, implementation, and enforcement of this policy. Exceptions to any provision of this policy must be formally requested through the Security Exception Request process (NT-SER-Form-01) and approved by the CISO or their delegate. All approved exceptions are logged in the Exception Register and reviewed quarterly.

---

2. Data Classification

2.1 Classification Levels

All information assets created, received, or maintained by NovaTech must be classified into one of four levels. Data owners are responsible for assigning the appropriate classification at the time of creation. Classification must be reviewed whenever the nature or sensitivity of the data changes.

Public: Information explicitly approved for external distribution. This includes marketing materials, published blog posts, press releases, and publicly available product documentation. Disclosure of Public data poses no risk to the Company.

Internal: Information intended for general use within NovaTech but not approved for external distribution. This includes internal communications, non-sensitive project documentation, organizational charts, internal process guides, and meeting notes that do not reference customer data. Unauthorized disclosure of Internal data could cause minor inconvenience but would not result in material harm.

Confidential: Information that, if disclosed without authorization, could cause significant harm to NovaTech or its customers. This includes customer data, financial records, employee personal data, proprietary source code, product roadmaps, pricing models, contract terms, audit reports, and security assessment results. Access to Confidential data is restricted to personnel with a documented business need.

Restricted: The most sensitive category of information. This includes authentication credentials, encryption keys, customer payment card data, health records, data subject to specific regulatory requirements (such as GDPR special category data), penetration test results, and incident response forensic evidence. Unauthorized disclosure of Restricted data could result in severe financial, legal, or reputational damage. Access is limited to specifically named individuals approved by the data owner and the CISO.

2.2 Data Classification Handling Requirements

The following table defines the minimum handling requirements for each classification level:

Requirement	Public	Internal	Confidential	Restricted
		Recommended		

Requirement	Public	Internal	Confidential	Restricted
Encryption at Rest	Not required		Required (AES-256)	Required (AES-256)
Encryption in Transit	TLS 1.2+	TLS 1.2+	TLS 1.3	TLS 1.3
Access Control	None	Role-based	Role-based + manager approval	Named-individual + CISO approval
Authentication	N/A	SSO	SSO + MFA	SSO + MFA + hardware token
Storage Locations	Any	Approved systems	Approved encrypted systems	Designated secure enclaves only
Sharing External	Permitted	NDA required	NDA + CISO approval	Prohibited except by CISO written authorization
Printing	Permitted	Permitted	Controlled (secure print)	Prohibited unless CISO-approved
Retention on Endpoints	Permitted	Permitted	Temporary only (max 30 days)	Prohibited
Backup Frequency	N/A	Weekly	Daily	Real-time replication
Disposal Method	Standard delete	Standard delete	Cryptographic erasure	Cryptographic erasure + audit log
Audit Logging	Not required	Basic access logs	Full access + modification logs	Full access + modification + read logs
Breach Notification	Not required	Internal only	CISO + Legal within 4 hours	CISO + Legal + CEO within 1 hour

2.3 Labeling

All documents and data stores containing Confidential or Restricted data must be clearly labeled with the appropriate classification. Digital documents must include the classification level in the header or footer. Email containing Confidential or Restricted data must include the classification in the subject line prefix (e.g., "[CONFIDENTIAL]"). Database tables and cloud storage buckets containing Confidential or Restricted data must be tagged accordingly in the asset management system.

---

3. Access Control

3.1 Principles

NovaTech enforces access control based on two foundational principles:

Role-Based Access Control (RBAC): Access rights are assigned to roles rather than individuals. Each employee is assigned one or more roles based on their job function. Roles are defined in the Identity and Access Management (IAM) system and map to specific sets of permissions across NovaTech systems. Standard roles include: Viewer, Contributor, Administrator, and System Owner. Custom roles require approval from the System Owner and the Security Team.

Principle of Least Privilege: Every user, service account, and automated process must operate with the minimum set of permissions necessary to perform its designated function. Permissions must not be granted on a speculative or convenience basis. When an employee's responsibilities change, their access rights must be adjusted within five business days.

3.2 Access Provisioning

Access requests are submitted through the IT Service Portal and must include: the system or resource requested, the business justification, the requested role or permission level, and the expected duration of access. All access requests for Confidential systems require manager approval. Access to Restricted systems additionally requires CISO approval and a completed background verification.

Temporary access (for contractors, project-based work, or cross-team collaboration) must include an expiration date. Temporary access grants may not exceed 90 days without renewal. Service accounts must be associated with a designated human owner who is responsible for the account's activity.

3.3 Quarterly Access Reviews

NovaTech conducts mandatory access reviews on a quarterly basis (Q1: January, Q2: April, Q3: July, Q4: October). During each review cycle:

1. System owners export a complete list of all user accounts and their assigned roles for each system they own.
2. Managers verify that each of their direct reports holds only the access rights necessary for their current role.
3. Any access rights that are no longer justified must be revoked within five business days of identification.
4. Dormant accounts (no login activity for 60 or more days) are flagged for review. Accounts dormant for 90 or more days are automatically disabled.
5. The Security Team audits a random sample of 15% of all access grants to verify compliance with RBAC policies.
6. Results are compiled into the Quarterly Access Review Report, which is presented to the CISO and retained for three years.

3.4 Privileged Access Management

Administrative and privileged accounts are subject to additional controls. All privileged access must be performed through the Privileged Access Management (PAM) platform, which enforces session recording, time-limited access windows, and just-in-time elevation. Privileged sessions are automatically terminated after 8 hours of continuous use. All privileged actions are logged and retained for a minimum of two years.

Standing administrative privileges are prohibited for production systems. Administrators must request elevated access through the PAM system for each session. Emergency break-glass accounts exist for critical system recovery scenarios and are secured with split-knowledge credentials held by the CISO and the VP of Engineering. Any use of break-glass accounts triggers an immediate notification to the Security Team and requires a post-incident review within 48 hours.

---

4. Incident Response

4.1 Overview

NovaTech maintains a structured incident response program to detect, contain, eradicate, and recover from security incidents in a timely and effective manner.

The Incident Response Team (IRT) consists of the CISO (Incident Commander), the Security Operations Lead, a designated Engineering Lead, a Communications Lead, and a Legal representative. The IRT may be supplemented with additional personnel as the nature of the incident requires.

4.2 Severity Levels

All security incidents are classified into one of four severity levels. The severity level determines the response timeline, escalation path, and communication requirements.

P1 — Critical: An active, ongoing breach involving confirmed unauthorized access to Restricted data, or a complete outage of production systems affecting all customers. Examples include: active exfiltration of customer payment data, ransomware encryption of production databases, or compromise of authentication infrastructure. P1 incidents require acknowledgment within 15 minutes of detection. The full Incident Response Team must be assembled within 30 minutes. The CEO, General Counsel, and Board Security Committee must be notified within 1 hour. External forensic support must be engaged within 2 hours if the scope of compromise is not fully determined. All other non-critical work by IRT members is immediately suspended for the duration of the P1 response.

P2 — High: A confirmed security incident with potential for significant impact but where active exploitation is contained or limited in scope. Examples include: unauthorized access to Confidential data with no evidence of exfiltration, a vulnerability being actively exploited in a non-production system, compromise of a single employee account with access to customer data, or detection of malware on internal systems that has not spread to production. P2 incidents require acknowledgment within 1 hour of detection. The Incident Commander and Security Operations Lead must be engaged within 1 hour. A preliminary impact assessment must be completed within 4 hours, which includes identifying all potentially affected systems, determining whether any customer data may have been accessed, and evaluating the attack vector. The Engineering Lead joins the response within 2 hours to begin technical containment. A status update must be provided to the CISO every 2 hours until the incident is downgraded or resolved. If the preliminary assessment indicates that customer data was accessed, the incident is automatically escalated to P1.

P3 — Medium: A security event that requires investigation but does not involve confirmed unauthorized access to sensitive data. Examples include: detection of anomalous but unconfirmed access patterns, a phishing email that was clicked but where no credentials were submitted, a misconfiguration discovered during

routine review that could have been exploited, or a failed brute-force attack against an employee account. P3 incidents require acknowledgment within 4 hours of detection. The Security Operations Lead assigns an analyst to investigate and determines whether escalation is warranted within 8 hours. A written summary must be delivered within 3 business days.

P4 — Low: A minor security event or policy violation with negligible immediate risk. Examples include: an employee sharing an Internal document without an NDA in place, a laptop with full-disk encryption reported lost, a single failed social engineering attempt that was recognized and reported, or a minor vulnerability discovered in a non-customer-facing internal tool. P4 incidents require acknowledgment within 24 hours. The Security Operations team investigates during normal business hours and documents findings within 5 business days.

4.3 Incident Response Procedures

All incidents, regardless of severity, follow the same six-phase response lifecycle:

Phase 1 — Detection and Reporting. Any employee who suspects a security incident must report it immediately through one of three channels: the Security Hotline (ext. 7700), the #security-incidents Slack channel, or email to security-alert@novatech.internal. Automated detection systems (SIEM, EDR, IDS) also generate alerts that are triaged by the Security Operations Center (SOC) during business hours and by the on-call analyst outside business hours.

Phase 2 — Triage and Classification. The receiving analyst performs initial triage to determine legitimacy and assigns a severity level (P1 through P4). The analyst documents the initial indicators, affected systems, and the time of detection in the Incident Tracking System. If severity is P1 or P2, the analyst immediately contacts the Incident Commander.

Phase 3 — Containment. The objective of containment is to limit the scope and impact of the incident. Containment actions vary by incident type but may include: isolating affected systems from the network, revoking compromised credentials, blocking malicious IP addresses or domains, disabling affected user accounts, or deploying emergency firewall rules. For P1 and P2 incidents, containment actions are authorized by the Incident Commander and must be documented in real time. The team distinguishes between short-term containment (immediate actions to stop ongoing damage) and long-term containment (measures to maintain business operations while preparing for eradication).

Phase 4 — Eradication. Once containment is achieved, the team identifies and eliminates the root cause. This may involve: removing malware, patching exploited vulnerabilities, rebuilding compromised systems from known-good images, rotating all potentially exposed credentials, and verifying that the attacker's access has been fully revoked. Eradication must be verified through independent validation — the analyst who performs eradication may not be the same individual who verifies its completeness.

Phase 5 — Recovery. Affected systems are restored to normal operation. Recovery actions are performed in a controlled manner, with monitoring increased on restored systems for a minimum of 72 hours following restoration. Customer-facing systems require sign-off from both the Engineering Lead and the Incident Commander before being returned to production. Recovery verification includes: confirming data integrity, validating that security controls are functioning correctly, and ensuring that no indicators of compromise remain.

Phase 6 — Post-Incident Review. A formal post-incident review is conducted for all P1 and P2 incidents within 5 business days of resolution. P3 incidents receive a written review within 10 business days. The review documents: the timeline of events, root cause analysis, effectiveness of the response, lessons learned, and specific remediation actions with assigned owners and deadlines. Post-incident review reports for P1 incidents are shared with the Board Security Committee. All post-incident reports are retained for five years.

4.4 Incident Communication

During P1 incidents, the Communications Lead issues an initial customer notification within 4 hours of confirmation that customer data was affected. Status updates are provided every 12 hours until resolution. For P2 incidents, customer communication is determined on a case-by-case basis by the Incident Commander in consultation with Legal.

---

5. Data Handling and Protection

5.1 Encryption Standards

All Confidential and Restricted data stored at rest must be encrypted using AES-256 or an equivalent algorithm approved by the Security Team. Encryption keys are managed through a centralized Key Management System (KMS) with automated rotation every 90 days. Key access is limited to the KMS administrators and is logged.

All data transmitted across networks — whether internal or external — must be encrypted using TLS 1.3 for Confidential and Restricted data. TLS 1.2 is the minimum acceptable standard for Internal and Public data transmission. Legacy protocols (SSL, TLS 1.0, TLS 1.1) are prohibited on all NovaTech systems. Certificate management is centralized, and all certificates must be issued by the NovaTech-approved Certificate Authority.

5.2 Data Retention and Disposal

NovaTech applies the following data retention schedule:

- **Active customer data:** Retained for the duration of the customer relationship and the contractual retention period thereafter (default: duration of the active subscription).
- **Deleted data:** When a customer or user deletes data through the application, the data is soft-deleted and recoverable for 30 days. After 30 days, the data enters a purge queue. All soft-deleted data is permanently purged within 90 days of the initial deletion request.
- **Backups:** Full system backups are retained for 1 year. Incremental backups are retained for 90 days. Backup media is encrypted using the same AES-256 standard applied to production data.
- **Logs and audit trails:** Security logs are retained for 2 years. Application logs are retained for 1 year. Access logs for Restricted data are retained for 3 years.
- **Employee data:** Retained for the duration of employment plus 3 years following termination, in accordance with applicable labor regulations.

When data reaches the end of its retention period, it must be disposed of using methods appropriate to its classification level as specified in the Data Classification Handling Requirements table (Section 2.2).

5.3 Data Loss Prevention

NovaTech deploys Data Loss Prevention (DLP) controls across email, cloud storage, and endpoint systems. DLP rules are configured to detect and block the unauthorized transmission of Confidential and Restricted data. DLP alerts are reviewed by the Security Operations team within 4 business hours. Confirmed violations are treated as security incidents and classified according to the severity framework in Section 4.2.

---

6. Acceptable Use Policy

6.1 General Principles

NovaTech provides information systems, devices, and network access to employees for the purpose of conducting authorized business activities. Limited personal use is permitted provided it does not interfere with work responsibilities, consume excessive resources, or violate any provision of this policy.

6.2 Prohibited Activities

The following activities are strictly prohibited on NovaTech systems and networks:

1. Accessing, downloading, storing, or transmitting illegal, obscene, or harassing material.
2. Attempting to gain unauthorized access to any system, account, or data — whether owned by NovaTech, its customers, or third parties.
3. Installing unauthorized software, including peer-to-peer file sharing applications, cryptocurrency miners, or unapproved browser extensions.
4. Disabling or circumventing security controls, including antivirus software, endpoint detection agents, firewalls, or DLP tools.
5. Sharing NovaTech credentials with any other person, including other NovaTech employees.
6. Using NovaTech systems to conduct business for any entity other than NovaTech without written authorization.
7. Connecting personal devices to the NovaTech production network. Personal devices may only access corporate resources through the approved Mobile Device Management (MDM) platform.
8. Transmitting Confidential or Restricted data through unapproved channels, including personal email accounts, unauthorized cloud storage services, or unencrypted messaging platforms.

6.3 Monitoring

NovaTech reserves the right to monitor, log, and audit all activity on Company-owned systems and networks. Employees should have no expectation of privacy when using NovaTech information systems. Monitoring data is classified as Confidential and is accessible only to the Security Team and authorized HR personnel in the context of an investigation.

---

7. Vendor Security Requirements

7.1 Vendor Risk Assessment

All third-party vendors who access, process, or store NovaTech data must complete a security assessment before engagement and annually thereafter. The depth of the assessment is determined by the classification of data the vendor will handle:

- **Vendors handling Public or Internal data:** Must complete the NovaTech Vendor Security Questionnaire (VSQ-Lite, 30 questions).
- **Vendors handling Confidential data:** Must complete the full NovaTech Vendor Security Questionnaire (VSQ-Full, 120 questions) and provide evidence of a SOC 2 Type II audit completed within the past 12 months.
- **Vendors handling Restricted data:** Must meet all Confidential-tier requirements plus undergo an on-site (or virtual) security audit conducted by the NovaTech Security Team.

7.2 Mandatory Certifications

SOC 2 Type II certification is mandatory for all vendors who process, store, or have access to customer data. Vendors must provide their most recent SOC 2 Type II report upon request and must notify NovaTech within 30 days of any material changes to the findings in their most recent report. Vendors who do not hold SOC 2 Type II certification may be granted a temporary exception (maximum 6 months) by the CISO, provided they present a documented remediation plan and agree to an enhanced monitoring program during the exception period.

7.3 Contractual Requirements

All vendor contracts involving access to Confidential or Restricted data must include: a data processing agreement (DPA) that specifies the scope and purpose of data processing, confidentiality obligations surviving termination by at least 3 years, a right-to-audit clause permitting NovaTech to conduct or commission security audits, mandatory breach notification within 48 hours, and data return or destruction requirements upon contract termination.

---

8. GDPR Compliance Procedures

8.1 Applicability

NovaTech processes personal data of individuals located in the European Economic Area (EEA) and the United Kingdom. As such, NovaTech complies with the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the UK GDPR. The Data Protection Officer (DPO) serves as the primary point of contact for all GDPR-related matters and can be reached at dpo@novatech.io.

8.2 Lawful Basis for Processing

NovaTech documents the lawful basis for every processing activity in the Record of Processing Activities (ROPA), maintained by the DPO. The most commonly relied upon bases are: contractual necessity (for processing required to deliver services to customers), legitimate interest (for internal analytics and service improvement, subject to a documented Legitimate Interest Assessment), and consent (for marketing communications and optional product features).

8.3 Data Subject Rights

NovaTech has established procedures to fulfill data subject rights requests within the GDPR-mandated timeframes:

1. **Right of Access (Article 15):** Data subjects may request a copy of their personal data. Requests are fulfilled within 30 days. If the request is complex or voluminous, a one-time 60-day extension may be applied with notification to the data subject.
2. **Right to Rectification (Article 16):** Inaccurate personal data is corrected within 15 business days of a verified request.
3. **Right to Erasure (Article 17):** Erasure requests are fulfilled within 30 days, subject to applicable legal retention requirements. Where erasure conflicts with a legal obligation, the data is restricted from further processing instead.
4. **Right to Data Portability (Article 20):** Personal data is provided in a machine-readable format (JSON or CSV) within 30 days of request.
5. **Right to Object (Article 21):** Processing for direct marketing purposes ceases within 5 business days of receiving an objection. Objections to processing based on legitimate interest are reviewed by the DPO within 15 business days.

All data subject requests are logged in the DSR Tracking System, and completion is verified by the DPO.

8.4 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is required before implementing any new processing activity that is likely to result in a high risk to the rights and freedoms of natural persons. Triggers for a mandatory DPIA include: large-scale processing of special category data, systematic monitoring of public areas, automated decision-making with legal or similarly significant effects, and processing of personal data involving new technologies. The DPO reviews all DPIA findings and escalates unresolved risks to the CISO and General Counsel.

---

9. Breach Notification

9.1 Internal Notification

Upon confirmation of a personal data breach, the Security Operations Lead must notify the DPO and the General Counsel within 2 hours. The DPO assesses whether the breach is likely to result in a risk to the rights and freedoms of natural persons and determines the notification obligations.

9.2 Regulatory Notification

Where a breach is determined to pose a risk to individuals, NovaTech will notify the relevant supervisory authority within 72 hours of becoming aware of the breach, in accordance with GDPR Article 33. The notification will include: the nature of the breach, the categories and approximate number of data subjects affected, the likely consequences, and the measures taken or proposed to address the breach. If full details are not available within 72 hours, NovaTech will provide information in phases without undue delay.

9.3 Notification to Affected Individuals

Where a breach is likely to result in a high risk to the rights and freedoms of affected individuals, NovaTech will notify those individuals without undue delay and no later than 7 days following the determination that individual notification is required. Notification will be provided through direct communication (email to the registered address) and will include: a description of the breach in clear and plain language, the name and contact details of the DPO, a description of the likely consequences, and a description of the measures taken to address the breach

and mitigate its effects. If direct notification is disproportionately difficult (e.g., contact details are unavailable), NovaTech will issue a public communication through its website and, where appropriate, social media channels.

9.4 Breach Register

All personal data breaches — regardless of whether they trigger notification obligations — are documented in the Breach Register maintained by the DPO. Each entry includes: the facts of the breach, its effects, and the remedial actions taken. The Breach Register is reviewed by the CISO and DPO monthly and is available for inspection by supervisory authorities upon request.

---

10. Training and Awareness

All NovaTech employees must complete the Information Security Awareness training within 30 days of joining the Company and annually thereafter. The training covers: data classification and handling, phishing recognition, password hygiene, incident reporting, and acceptable use. Employees with access to Confidential or Restricted data must additionally complete the Advanced Data Handling module. Completion rates are tracked by the People Operations team and reported to the CISO quarterly. Employees who fail to complete mandatory training within the required timeframe will have their system access suspended until training is completed.

---

11. Enforcement and Compliance

Violations of this policy may result in disciplinary action up to and including termination of employment or contract. Serious violations may also result in civil or criminal liability. The Security Team conducts periodic compliance audits to verify adherence to this policy. Audit findings are reported to the CISO and, for material findings, to the Executive Leadership Team.

Employees are encouraged to report suspected violations through the confidential Ethics Hotline or directly to the Security Team. NovaTech prohibits retaliation against any individual who reports a suspected violation in good faith.

---

12. Document Control

Version	Date	Author	Changes
1.0	March 1, 2022	M. Chen, CISO	Initial release
2.0	January 15, 2023	M. Chen, CISO	Added GDPR procedures, vendor requirements
3.0	January 15, 2024	S. Patel, CISO	Revised incident severity levels, updated encryption standards to TLS 1.3
3.1	July 15, 2024	S. Patel, CISO	Updated data retention schedule, added PAM requirements
3.2	January 15, 2025	S. Patel, CISO	Updated vendor SOC 2 requirements, revised breach notification timelines

---