Data Classification Policy

Document ID: IT-SEC-005 **Last Updated:** 2024-02-01 **Owner:** Security Team **Classification:** Internal

---

Purpose

This policy establishes NovaTech's data classification framework to ensure appropriate protection of information assets based on sensitivity and regulatory requirements.

Classification Levels

Level 1: Public

Definition: Information intended for public distribution with no negative impact if disclosed.

Examples: - Marketing materials - Public website content - Press releases - Open source code - Published blog posts

Handling: - No restrictions on sharing - May be posted publicly - No encryption required

---

Level 2: Internal

Definition: Information intended for internal use that could cause minor impact if disclosed externally.

Examples: - Internal policies and procedures - Organization charts - Internal communications - Non-sensitive meeting notes - Training materials

Handling: - Share only with NovaTech employees - Do not post publicly - May be shared via internal tools (Slack, Notion, email) - No external sharing without approval

---

Level 3: Confidential

Definition: Sensitive information that could cause significant harm if disclosed. Requires need-to-know access.

Examples: - Customer data (non-PII) - Business strategies and plans - Financial reports (non-public) - Vendor contracts - Technical architecture details - Security configurations - Employee personal information

Handling: - Access limited to those with business need - Encrypt in transit and at rest - Do not share externally without NDA - Do not store on personal devices - Secure disposal required

---

Level 4: Restricted

Definition: Highly sensitive information that could cause severe harm if disclosed. Strictest controls apply.

Examples: - Customer PII (names, emails, addresses) - Payment card data (PCI) - Healthcare data (HIPAA) - Authentication credentials - Encryption keys - Security vulnerabilities (unpatched) - Legal matters - M&A information

Handling: - Strict need-to-know access - Strong encryption required - Access logged and audited - No external sharing without legal approval - Formal access request process - Secure destruction required

---

Classification by Data Type

Data Type	Classification	Notes
Customer usage data (aggregated)	Internal	Anonymized analytics
Customer usage data (individual)	Confidential	Identifiable patterns
Customer PII	Restricted	Names, emails, etc.
Customer financial data	Restricted	Payment, billing
Source code (proprietary)	Confidential	Core IP

Data Type	Classification	Notes
Source code (open source)	Public	Published repos
Employee directory	Internal	Names, titles
Employee HR records	Restricted	Compensation, reviews
Security logs	Confidential	Incident investigation
Credentials/secrets	Restricted	API keys, passwords
Public financials	Public	Published reports
Internal financials	Confidential	Management reports
Board materials	Restricted	Board deck, minutes

Handling Requirements

Storage

Classification	Approved Storage
Public	Any
Internal	Google Drive, Notion, Slack, Company systems
Confidential	Google Drive (Team Drives), Approved databases, Encrypted systems
Restricted	Encrypted databases, Vault, Approved secure storage only

Transmission

Classification	Requirements
Public	No restrictions
Internal	Internal systems or encrypted external
Confidential	Encrypted channels only (TLS, encrypted email)
Restricted	Encrypted + verified recipient + logged

Retention

Classification	Default Retention
Public	No limit
Internal	7 years or business need
Confidential	Per legal/compliance requirements
Restricted	Minimum necessary, per compliance

Disposal

Classification	Method
Public	Standard deletion
Internal	Standard deletion
Confidential	Secure deletion, device wipe
Restricted	Certified destruction, documented

Labeling Requirements

Documents

- Restricted: Must be labeled "RESTRICTED - [Category]"
- Confidential: Should be labeled "CONFIDENTIAL"
- Internal: Optional label "INTERNAL"
- Public: No label required

Emails

- Restricted: Subject prefix "[RESTRICTED]"
- Confidential: Subject prefix "[CONFIDENTIAL]" recommended

Systems

- Databases containing Restricted data must be tagged in inventory
- Cloud resources labeled per classification level

Access Control

Principles

- **Least Privilege:** Minimum access necessary for job function
- **Need-to-Know:** Access only to required information
- **Segregation:** Separate conflicting duties

Access Requests

Classification	Approval Required
Public	None
Internal	Manager
Confidential	Manager + Data Owner
Restricted	Manager + Data Owner + Security

Access Reviews

- Restricted: Quarterly
- Confidential: Semi-annually
- Internal: Annually

Special Categories

Personal Data (GDPR/CCPA)

All personal data is minimum Confidential: - Requires documented lawful basis - Subject to data subject rights - 72-hour breach notification (GDPR) - See Privacy Policy for details

Payment Card Data (PCI)

All payment data is Restricted: - PCI-DSS compliance required - Stored only in certified systems - Access strictly limited - Annual compliance validation

Health Data (HIPAA)

If NovaTech handles PHI: - Minimum Restricted classification - HIPAA compliance required - BAA required with partners

---

Incident Response

Classification-Related Incidents

Incident	Response
Mislabeled data	Correct immediately, assess exposure
Unauthorized access	Report to Security, investigate
Data breach (Restricted)	Immediate escalation, follow IR plan
External disclosure	Legal notification, damage assessment

Reporting

Report classification incidents to: - security@novatech.com - #security-urgent (Slack)

Training

Required Training

- All employees: Annual data classification training
- Data handlers: Role-specific training
- Administrators: Detailed classification training

Resources

- Classification decision guide (wiki)
- Data handling quick reference card
- Security team consultation

Responsibilities

Data Owners

- Assign appropriate classification
- Approve access requests
- Review access periodically
- Ensure proper handling

Employees

- Handle data according to classification
- Report suspected misclassification
- Complete required training
- Follow disposal procedures

Security Team

- Maintain classification framework
- Audit compliance
- Investigate incidents
- Provide guidance

Exceptions

Exceptions require written approval: - Confidential: Security Manager - Restricted: CISO

Document business justification and compensating controls.

Related Documents: Security Best Practices (IT-SEC-010), Privacy Policy (COM-DP-002), Incident Response Plan (IT-SEC-020)