Data Classification Policy

Document ID: IT-SEC-015 **Last Updated:** March 2024 **Owner:** Information Security **Applies To:** All Employees

---

Overview

NovaTech's data classification policy establishes standards for categorizing, handling, and protecting company data based on sensitivity levels. All employees are responsible for properly classifying and handling data according to this policy.

Classification Levels

Public

Definition: Information intended for public consumption with no restrictions on disclosure.

Examples: - Marketing materials - Published blog posts - Public product documentation - Press releases - Open source code

Handling Requirements: - No special handling required - May be shared externally without approval - May be stored on any approved system

Label: `Public` or no label required

Internal

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

Examples: - Internal communications - Non-sensitive policies - Organization charts - Internal documentation - Project plans - Meeting notes (non-sensitive)

Handling Requirements: - Default classification for most internal content - May be shared with employees and contractors - Must not be shared externally without approval - Store on approved internal systems

Label: `Internal` or `NovaTech Internal`

Confidential

Definition: Sensitive information that could cause significant harm to NovaTech or individuals if disclosed.

Examples: - Financial data and projections - Customer lists and contracts - Strategic plans - Employee personal information - Unpublished product roadmaps - Competitive analysis - Salary information - Security configurations

Handling Requirements: - Encryption required at rest and in transit - Access limited to need-to-know basis - Approval required for external sharing - Must not be stored on personal devices - Audit logging required - Secure disposal required

Label: `Confidential`

Restricted

Definition: Highly sensitive information that could cause severe harm if disclosed. Includes regulated data.

Examples: - Authentication credentials and secrets - Customer PII (when bulk or sensitive) - Customer PHI (health information) - Payment card data (PCI) - Encryption keys - Security vulnerabilities (unpatched) - M&A information - Legal holds

Handling Requirements: - Encryption required (AES-256 or equivalent) - Strict access controls with MFA - VP or above approval for any sharing - No external sharing without Legal approval - No local storage - approved systems only - Full audit trail required - Immediate incident reporting if exposed - Secure disposal with verification

Label: `Restricted` or `Highly Confidential`

Classification Matrix

Data Type	Classification	Owner
Marketing content	Public	Marketing
Public docs	Public	Product
Internal wiki	Internal	All
Project plans	Internal	PMO
Financial reports	Confidential	Finance
Customer contracts	Confidential	Legal
Employee records	Confidential	HR

Data Type	Classification	Owner
Strategic plans	Confidential	Executive
Source code	Confidential	Engineering
Customer PII	Restricted	Security
Payment data	Restricted	Finance
API keys/secrets	Restricted	Engineering
Security reports	Restricted	Security

Handling Guidelines

Storage

Classification	Approved Storage
Public	Any approved system
Internal	Google Drive, Confluence, Slack
Confidential	Google Drive (encrypted), Confluence (restricted), SecureVault
Restricted	SecureVault, Encrypted DB, Approved cloud with encryption

Transmission

Classification	Email	Slack	External
Public			
Internal			With approval
Confidential	Encrypted only	Private channels	VP approval
Restricted	Not allowed	Not allowed	Legal approval

Sharing

Classification	Internal Sharing	External Sharing
Public	Open	Open
Internal	All employees	Manager approval
Confidential	Need-to-know	VP + Legal approval
Restricted	Explicit authorization	C-level + Legal

Labeling Requirements

Document Labels

Apply labels to all documents:

Header/Footer format:

```
Classification: [Level]
Owner: [Department]
```

File naming convention:

```
[CLASSIFICATION]_filename.ext
Example: CONFIDENTIAL_Q3_financials.xlsx
```

Email Labels

Include classification in subject line for Confidential and above:

```
Subject: [CONFIDENTIAL] Q3 Financial Review
```

Slack Messages

Use channel descriptions and pinned messages for classification:

```
Channel Topic: [CONFIDENTIAL] - Finance discussions only
```

Roles and Responsibilities

Data Owners

- Determine classification level
- Approve access requests
- Review classification periodically
- Ensure proper handling by users

All Employees

- Classify data you create
- Handle data according to classification
- Report misclassification or exposure
- Complete classification training

IT/Security

- Provide tools for classification
- Enforce technical controls
- Monitor compliance
- Investigate incidents

Managers

- Ensure team compliance
- Approve Internal data sharing
- Review access periodically
- Support classification training

Classification Process

New Data

1. **Identify** the data type and content
2. **Assess** potential harm if disclosed
3. **Classify** according to definitions
4. **Label** appropriately
5. **Store** in approved location
6. **Control** access based on classification

Existing Data

1. Review data during regular audits
2. Reclassify if conditions change
3. Update labels and controls
4. Notify affected users of changes

Reclassification

Data may need reclassification when: - Information becomes public - Sensitivity increases - Regulatory requirements change - Time-based restrictions expire

Process: 1. Data owner assesses change 2. Security reviews if upgrading 3. Update labels and controls 4. Communicate to stakeholders

---

Technical Controls

Encryption Requirements

Classification	At Rest	In Transit
Public	Optional	TLS recommended
Internal	Recommended	TLS required
Confidential	Required (AES-256)	TLS 1.2+ required
Restricted	Required (AES-256)	TLS 1.2+ with PFS

Access Controls

Classification	Authentication	Authorization
Public	None	None
Internal	SSO	Role-based
Confidential	SSO + MFA	Need-to-know
Restricted	SSO + MFA	Explicit approval

Monitoring

Classification	Logging	Alerting
Public	Basic	None
Internal	Access logs	Anomalies
Confidential	Full audit	Suspicious access
Restricted	Full audit + DLP	All access

Compliance Requirements

SOC 2

- Data classification documented
- Access controls implemented
- Encryption standards defined

GDPR

- Personal data identified
- Processing purposes documented
- Data minimization applied

HIPAA

- PHI identified and classified
- Minimum necessary standard
- Business associate requirements

PCI-DSS

- Cardholder data identified
- Storage and transmission secured
- Access restricted

Exceptions

Exception Process

1. Submit exception request to Security
2. Provide business justification
3. Identify compensating controls
4. Security team reviews
5. Approval documented
6. Exception expires in 12 months max

Common Exceptions

- Temporary storage during migration
- Legacy system limitations
- Third-party integration requirements
- Customer contractual requirements

Training Requirements

All Employees

- Annual data classification training
- Pass assessment with 80%+ score
- Acknowledge policy annually

Data Owners

- Additional owner-specific training
- Classification decision workshop
- Annual refresher

Technical Staff

- Technical controls training
- DLP and encryption tools
- Incident response procedures

Incident Response

Suspected Exposure

If you suspect data has been misclassified or exposed:

1. **Stop** - Don't forward or spread the data
2. **Report** - Contact security@novatech.com immediately
3. **Document** - Note what happened and when
4. **Preserve** - Don't delete evidence

Security Team Response

For Confidential or Restricted data exposure:

1. Assess scope and impact
2. Contain exposure
3. Notify affected parties
4. Remediate and prevent recurrence
5. Document and report

Resources

- **Classification Training:** learn.novatech.com/data-classification
- **DLP Tools:** Configured in Google Workspace
- **Questions:** security@novatech.com
- **Slack:** #security-questions

Related Documents

- Information Security Policy (IT-SEC-001)
- Acceptable Use Policy (IT-SEC-005)
- Incident Response Plan (IT-SEC-020)
- Data Retention Policy (IT-SEC-025)

Review Cycle: Annual Next Review: March 2025