Data Retention Policy

Document ID: COM-DP-005 **Last Updated:** 2024-01-20 **Owner:** Legal & Compliance **Classification:** Internal

---

Purpose

This policy establishes NovaTech's requirements for retaining and disposing of data. Proper data retention ensures compliance with legal obligations, supports business operations, and minimizes risk.

Scope

This policy applies to: - All NovaTech employees, contractors, and vendors - All data created, received, or maintained by NovaTech - All storage systems (electronic and physical)

Retention Principles

Keep Only What's Necessary

- Retain data only as long as required
- Delete data when retention period expires
- Minimize collection of unnecessary data

Legal Compliance First

- Legal requirements override business preferences
- Litigation holds suspend normal retention
- Regulatory requirements vary by data type

Consistent Application

- Apply retention schedules uniformly
- Document exceptions
- Regular audits ensure compliance

Retention Schedule

Customer Data

Data Type	Retention Period	Justification
Account information	Duration of relationship + 7 years	Tax, legal
Transaction records	7 years	Tax, audit
Support tickets	3 years after resolution	Quality, legal
Usage/analytics data	2 years	Product improvement
Marketing preferences	Duration of consent	GDPR/CCPA

Employee Data

Data Type	Retention Period	Justification
Personnel files	Employment + 7 years	Legal, tax
Payroll records	7 years	Tax, audit
I-9 forms	3 years after hire or 1 year after termination	Immigration law
Performance reviews	Employment + 3 years	Legal
Benefits records	6 years after plan year	ERISA
Recruitment records	3 years	EEOC
Training records	Employment + 5 years	Compliance

Business Records

Data Type	Retention Period	Justification
Contracts	Expiration + 7 years	Legal
Financial statements	Permanent	Corporate
Tax returns	7 years	Tax
Board minutes	Permanent	Corporate
Insurance policies	Policy term + 10 years	Claims
Vendor records	Relationship + 7 years	Tax, legal

Technical Data

Data Type	Retention Period	Justification
System logs	90 days	Security, debugging
Security logs	2 years	Compliance, forensics
Audit logs	7 years	Compliance
Backups	90 days (rolling)	Recovery
Source code	Permanent	Business continuity
Incident reports	7 years	Legal, analysis

Communications

Data Type	Retention Period	Justification
Email (general)	3 years	Business operations
Email (legal/HR)	7 years	Legal
Slack messages	2 years	Business operations
Meeting recordings	1 year	Business operations
Voicemail	90 days	Business operations

Retention by Regulation

GDPR (EU Data)

- Personal data: Only as long as necessary for stated purpose
- Consent records: Duration of processing + 3 years
- Data subject requests: 6 years

CCPA (California Data)

- Consumer requests: 24 months
- Opt-out records: Indefinitely
- Training records: 24 months

SOC 2

- Audit evidence: 7 years
- Security logs: 1 year minimum
- Policy documents: Current + 1 version

HIPAA (If Applicable)

- Medical records: 6 years from creation or last effective date
- HIPAA-related documents: 6 years

PCI-DSS

- Cardholder data: Only as needed for transaction
- Audit logs: 1 year (3 months immediately available)

Litigation Hold

When Triggered

- Litigation is filed or reasonably anticipated
- Government investigation
- Regulatory inquiry
- Internal investigation

Hold Process

1. Legal issues hold notice
2. Identifies affected data types and custodians
3. Normal deletion suspended
4. Affected parties must preserve all relevant data
5. Hold remains until lifted by Legal

Responsibilities

- **Legal:** Issue and manage holds
- **IT:** Implement technical holds
- **Custodians:** Preserve data, report compliance
- **All:** Do not delete data under hold

Disposal Procedures

Electronic Data

Standard Data: - Logical deletion from production - Removal from backups after retention period

Sensitive Data: - Secure deletion using approved tools - Certificate of destruction for regulated data

Storage Media: - Secure wipe before reuse (NIST 800-88) - Physical destruction for end-of-life

Physical Records

Standard Documents: - Cross-cut shredding - Secure recycling bins

Sensitive Documents: - On-site shredding by approved vendor - Certificate of destruction

Schedule: - Quarterly disposal review - Annual physical destruction event

---

Implementation

Data Classification

All data should be classified to determine retention:

Classification	Retention Guidance
Public	No mandatory retention
Internal	Per business schedule
Confidential	Per regulation/contract
Restricted	Strictest applicable requirement

Systems and Tools

Automated Retention: - Email archiving (retention rules applied automatically) - Cloud storage (lifecycle policies) - Database purge jobs

Manual Retention: - Shared drives (annual review) - Physical records (scheduled destruction)

Exceptions

Request exceptions via: 1. Submit to Legal with business justification 2. Legal reviews against obligations 3. Approved exceptions documented 4. Annual exception review

---

Roles and Responsibilities

Legal Team

- Maintain retention schedule
- Issue litigation holds
- Approve exceptions
- Respond to regulatory inquiries

IT Team

- Implement technical retention controls
- Execute secure disposal
- Maintain backup schedules
- Support litigation holds

Data Owners

- Apply retention to their data
- Review data annually
- Respond to hold requests
- Report exceptions

All Employees

- Follow retention requirements
- Do not delete data under hold
- Report retention concerns
- Complete required training

Monitoring and Audit

Regular Reviews

- Annual retention schedule review
- Quarterly disposal execution
- Monthly backup verification

Audits

- Annual internal audit of retention compliance
- External audit as part of SOC 2
- Sample-based verification

Metrics

- Percentage of data with retention applied
- Litigation hold compliance rate
- Disposal completion rate

Violations

Failure to follow this policy may result in: - Disciplinary action - Legal liability - Regulatory penalties - Reputation damage

Report violations to legal@novatech.com or via anonymous ethics hotline.

Training

All employees must complete: - Initial retention training (onboarding) - Annual refresher training - Litigation hold training (when issued)

Related Documents: Data Classification Policy (IT-SEC-005), GDPR Compliance Guide (COM-DP-001), Information Security Policy (IT-SEC-001)