Data Breach Response Plan

Document ID: COM-DP-015 **Effective Date:** January 1, 2024 **Last Updated:** February 2024 **Owner:** Information Security & Legal **Classification:** Internal

---

Purpose

This plan establishes procedures for identifying, containing, and responding to data breaches involving personal or sensitive information.

Scope

This plan covers: - Personal data breaches (customer, employee, partner) - Confidential business information breaches - All NovaTech systems and data

---

Definition of Data Breach

A data breach is an incident where: - Personal data is accessed without authorization - Data is lost, stolen, or destroyed - Data is disclosed to unauthorized parties - Data integrity is compromised

Examples

Confirmed breaches: - Ransomware encrypting customer data - Employee credentials phished, data accessed - Laptop with unencrypted data stolen - Database exposed to internet - Unauthorized data export

Potential breaches (require investigation): - Suspicious login from unusual location - Unexpected data access patterns - Lost device with encrypted data - Phishing email clicked, unclear if data accessed

---

Breach Response Team

Core Team

Role	Primary	Backup
Incident Commander	CISO	VP Engineering
Legal Lead	General Counsel	Outside Counsel
Communications Lead	VP Marketing	CEO
Technical Lead	Security Manager	SRE Lead
HR Lead (if employee data)	CPO	HR Director
Customer Lead	VP Customer Success	Director Support

Extended Team (as needed)

- External forensics firm
- Crisis communications agency
- Outside legal counsel
- Law enforcement liaison
- Insurance carrier

Response Phases

Phase 1: Detection & Initial Response (0-2 hours)

Objectives: - Confirm breach occurred - Contain immediate damage - Preserve evidence - Activate response team

Actions:

1. **Confirm the breach**
    - Gather initial information
    - Determine if data was actually accessed/exfiltrated
    - Identify affected systems
2. **Contain the breach**
    - Isolate affected systems
    - Revoke compromised credentials
    - Block malicious IPs/actors
    - DO NOT destroy evidence
3. **Preserve evidence**

- Create forensic images
- Preserve logs
- Document all actions taken
- Maintain chain of custody

4. **Activate response team**
   - Notify Incident Commander
   - Establish communication channel (dedicated Slack)
   - Schedule initial briefing
   - Engage external resources if needed

Phase 2: Assessment (2-24 hours)

Objectives: - Determine scope and impact - Identify affected data and individuals - Assess notification requirements

Actions:

1. **Scope determination**
   - What data was affected?
   - How many records?
   - What systems?
   - What time period?
2. **Data classification**
   - Personal data (names, emails)?
   - Sensitive personal data (SSN, financial)?
   - Health information (HIPAA)?
   - Payment card data (PCI)?
   - Business confidential?
3. **Impact assessment**
   - Number of affected individuals
   - Geographic locations (regulatory implications)
   - Risk to individuals
   - Business impact
4. **Root cause analysis**
   - How did the breach occur?
   - What vulnerabilities were exploited?
   - Was it intentional or accidental?

Phase 3: Notification (24-72 hours)

Objectives: - Meet legal notification requirements - Inform affected parties appropriately - Maintain transparency

Legal Requirements:

Regulation	Timing	Threshold
GDPR	72 hours	Risk to individuals
CCPA	Without delay	500+ CA residents
State laws	Varies (30-90 days)	Varies
HIPAA	60 days	Unsecured PHI
PCI DSS	Immediately	Card data

Notification Steps:

1. **Regulatory notification**
   - GDPR: Supervisory authority within 72 hours
   - Other regulators per requirements
   - Legal coordinates timing
2. **Individual notification**
   - Clear description of what happened
   - Types of data involved
   - Steps we're taking
   - Steps they can take
   - Contact information
3. **Customer notification**
   - For B2B: Notify affected customers
   - Support customer's own notification needs
   - Provide incident details per contract
4. **Other notifications**
   - Insurance carrier
   - Law enforcement (if criminal)
   - Board of directors
   - Partners (if affected)

Phase 4: Remediation (Ongoing)

Objectives: - Fix vulnerabilities - Restore normal operations - Prevent recurrence

Actions:

1. **Technical remediation**
    - Patch vulnerabilities
    - Strengthen controls
    - Enhance monitoring
    - Restore from clean backups
2. **Process improvements**
    - Update policies
    - Enhance training
    - Improve detection
3. **Support for affected individuals**
    - Credit monitoring (if appropriate)
    - Identity protection services
    - Dedicated support channel

Phase 5: Post-Incident Review (1-2 weeks after)

Objectives: - Document lessons learned - Improve response capabilities - Prevent future incidents

Actions:

1. **Post-mortem meeting**
    - Timeline review
    - What went well
    - What could improve
    - Action items
2. **Documentation**
    - Complete incident report
    - Update response plan
    - File with legal/compliance
3. **Communication**
    - Final customer communication
    - Internal lessons learned
    - Board update

Communication Templates

Internal Initial Notification

```
SECURITY INCIDENT - CONFIDENTIAL

A potential data breach has been identified.

Time detected: [TIME]
Systems affected: [SYSTEMS]
Initial assessment: [BRIEF DESCRIPTION]

Response team has been activated. Updates will be provided via [CHANNEL].

DO NOT discuss this incident outside of [CHANNEL].
DO NOT communicate with external parties without approval.
DO NOT take actions that may destroy evidence.

Contact: [INCIDENT COMMANDER]
```

Customer Notification Template

```
Subject: Important Security Notice from NovaTech

Dear [Customer],

We are writing to inform you of a security incident that may have affected your information.

What Happened:
[Clear, factual description]

What Information Was Involved:
[Types of data affected]

What We Are Doing:
[Actions taken and planned]

What You Can Do:
[Recommended steps for customer]

For More Information:
[Contact details, FAQ link]

We sincerely apologize for any inconvenience and are committed to protecting your informatio
```

```
[Signature]
```

Regulatory Notification (GDPR)

```
PERSONAL DATA BREACH NOTIFICATION

To: [Supervisory Authority]
From: NovaTech Solutions, Inc.
Date: [DATE]
DPO Contact: dpo@novatech.com

Nature of breach: [Description]
Categories of data: [Types]
Approximate records: [Number]
Likely consequences: [Assessment]
Measures taken: [Actions]
Contact for questions: [Contact info]

[Full details attached]
```

Documentation Requirements

During Incident

Document: - All actions taken - Timeline of events - Decisions made and rationale - Communications sent - Evidence preserved

Post-Incident

Prepare: - Complete incident report - Forensics report (if applicable) - Notification records - Lessons learned document - Updated procedures

Retention

- Incident documentation: 7 years
- Forensic evidence: Per legal hold
- Communication records: 7 years

Testing and Training

Tabletop Exercises

- Conduct quarterly
- Involve all response team members
- Test different scenarios
- Document findings and improvements

Training

- Annual breach response training
- Role-specific training for response team
- New employee awareness

Plan Review

- Annual review (minimum)
- After each incident
- When regulations change
- When organization changes

Contact Information

Internal

Role	Contact
Security	security@novatech.com
Legal	legal@novatech.com
HR	hr@novatech.com
DPO	dpo@novatech.com

External

Resource	Contact
Outside Counsel	[Firm name, contact]
Forensics Firm	[Firm name, contact]
PR Agency	[Agency name, contact]

Resource	Contact
Cyber Insurance	[Carrier, policy number]

Regulatory

Authority	Contact
ICO (UK)	ico.org.uk
CNIL (France)	cnil.fr
State AGs	Per state

Related Documents: Incident Response Plan (IT-SEC-010), Privacy Policy (COM-DP-010), Security Best Practices (IT-SEC-001)