INCIDENT RESPONSE POLICY

Company: Convo, Inc.
Effective Date: September 1st, 2025 **Version:** 1.0
Owner: Security Team (markus@itsconvo.com)
Review Frequency: Annually

---

1. PURPOSE AND SCOPE

1.1 Purpose

This policy establishes procedures for detecting, responding to, and recovering from security incidents that may affect the confidentiality, integrity, or availability of customer data, systems, or services.

1.2 Scope

This policy applies to:

- All Convo systems, applications, and infrastructure
- All customer data and Personal Data processed by Convo
- All employees, contractors, and third-party service providers
- All security incidents, including but not limited to data breaches, system compromises, and service disruptions

1.3 Definitions

- **Security Incident:** Any actual or suspected breach of security that compromises the confidentiality, integrity, or availability of data or systems
- **Personal Data Breach:** A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to Personal Data
- **Critical Incident:** An incident with high impact on customer data, service availability, or regulatory compliance
- **Major Incident:** An incident with moderate impact requiring immediate attention
- **Minor Incident:** An incident with low impact that can be handled through standard procedures

---

2. INCIDENT RESPONSE TEAM

2.1 Core Team Structure

Role	Responsibilities	Primary Contact	Backup
Incident Commander	Overall incident coordination, decision making	Ivan (COO)	Markus Kellermann (CTO)
Security Lead	Technical investigation, containment	[Security Engineer]	[DevOps Lead]
Communications Lead	Customer/stakeholder communication	[Customer Success]	Ivan
Legal/Compliance	Regulatory requirements, legal implications	[Legal Contact]	External Counsel
Technical Lead	System recovery, technical remediation	[CTO/Lead Developer]	[Senior Developer]

2.2 Extended Team (On-Call)

- Customer Success Manager
- DevOps Engineer
- External Security Consultant
- Legal Counsel (External)
- Public Relations (if needed)

---

3. INCIDENT CLASSIFICATION

3.1 Classification Matrix

Level	Impact	Examples	Response Time
Critical	High customer/data impact	Personal data breach, system compromise, complete service outage	15 minutes
Major	Moderate impact	Partial service degradation, suspected breach, significant vulnerability	1 hour
Minor	Low impact	Failed login attempts, minor system alerts, low-risk vulnerabilities	4 hours

3.2 Personal Data Breach Classification

Automatic Critical if incident involves:

- Unauthorized access to Personal Data
- Loss or theft of devices containing Personal Data
- Accidental disclosure of Personal Data
- Ransomware or malware affecting systems with Personal Data
- Any incident affecting >100 data subjects

---

4. DETECTION AND REPORTING

4.1 Detection Methods

- **Automated Monitoring:** Security alerts from SIEM, IDS, and monitoring tools
- **Employee Reports:** Internal team members reporting suspicious activity
- **Customer Reports:** Customers reporting potential security issues
- **Third-Party Notifications:** Vendors, partners, or security researchers
- **Audit Findings:** Internal or external audit discoveries

4.2 Internal Reporting

All employees must immediately report suspected incidents via:

- **Primary:** markus@itsconvo.com
- **Phone:** [24/7 Security Hotline]
- **Slack:** #security-incidents channel
- **Emergency:** Direct call to Incident Commander

4.3 Reporting Information Required

- Date and time of discovery
- Description of the incident
- Systems or data potentially affected
- Actions already taken (if any)
- Contact information of person reporting

---

5. RESPONSE PROCEDURES

5.1 Initial Response (0-15 minutes)

1. **Incident Commander Activation**
   - Receive incident notification
   - Perform initial classification (Critical/Major/Minor)

- Activate incident response team based on severity
- Establish incident communication channel

2. **Immediate Assessment**
   - Verify incident legitimacy
   - Assess scope and potential impact
   - Determine if Personal Data is involved
   - Document initial findings

5.2 Containment (15 minutes - 1 hour)

1. **Immediate Containment**
   - Isolate affected systems to prevent spread
   - Preserve evidence for investigation
   - Implement temporary security measures
   - Monitor for additional compromise
2. **System Stabilization**
   - Ensure service continuity where possible
   - Implement workarounds for critical services
   - Monitor system performance and security

5.3 Investigation (1-24 hours)

1. **Forensic Analysis**
   - Collect and analyze logs
   - Determine root cause
   - Assess full scope of compromise
   - Identify attack vectors and timeline
2. **Impact Assessment**
   - Determine data affected (types, volumes, sensitivity)
   - Identify affected customers and data subjects
   - Assess potential harm to individuals
   - Document evidence chain of custody

5.4 Eradication and Recovery (24-72 hours)

1. **Threat Elimination**
   - Remove malicious code/access
   - Close attack vectors
   - Apply security patches
   - Update security controls
2. **System Recovery**
   - Restore affected systems from clean backups
   - Verify system integrity
   - Implement additional monitoring
   - Conduct security testing

5.5 Communication Timeline

Timeframe	Internal	Customer	Regulatory
0-1 hour	Team notification	None (unless ongoing impact)	None
1-4 hours	Status update	Major customers if service impact	None
4-24 hours	Full team briefing	Affected customers if confirmed breach	None yet
24-72 hours	Recovery status	All affected customers	GDPR notification if required

---

6. CUSTOMER COMMUNICATION

6.1 Communication Principles

- **Transparency:** Provide accurate, timely information
- **Empathy:** Acknowledge impact and concerns
- **Action-Oriented:** Clearly state what we're doing and what they should do
- **Follow-up:** Regular updates until resolution

6.2 Communication Templates

Initial Customer Notification (Critical Incidents)

```
Subject: Important Security Notice - Immediate Action Required

Dear [Customer],

We are writing to inform you of a security incident affecting our systems that may have impa

**What Happened:**
[Brief description of incident]

**Data Potentially Affected:**
[Specific data types and approximate numbers]

**What We're Doing:**
- Immediately contained the incident
- Launched full investigation with external security experts
- Implemented additional security measures
- Working with law enforcement as appropriate
```

```
**What You Should Do:**
[Specific recommended actions]

**Next Steps:**
We will provide updates every [frequency] until this matter is resolved.

Contact: markus@itsconvo.com

Sincerely,
Markus Kellermann, CEO
```

6.3 Customer Communication Matrix

Incident Level	Who to Notify	When	Method
Critical	All affected customers	Within 24 hours of confirmation	Email + Phone call
Major	Affected customers	Within 72 hours	Email
Minor	No proactive notification	Not applicable	Available upon request

---

7. REGULATORY NOTIFICATION

7.1 GDPR Requirements (EU Customers)

Supervisory Authority Notification:

- **Timeline:** Within 72 hours of becoming aware
- **Method:** Online notification to relevant Data Protection Authority
- **Content:** Nature of breach, affected data subjects, likely consequences, measures taken

Data Subject Notification:

- **Timeline:** Without undue delay if high risk to rights and freedoms
- **Method:** Direct communication (email, letter, or public communication if impractical)
- **Content:** Nature of breach, likely consequences, measures taken, contact information

7.2 Other Regulatory Requirements

- **US State Laws:** California (CCPA), New York (SHIELD Act) - 72 hours to Attorney General
- **Sector-Specific:** HIPAA (60 days), PCI DSS (immediately to payment brands)
- **Customer Contractual:** Per individual customer agreements

---

8. DOCUMENTATION REQUIREMENTS

8.1 Incident Documentation

All incidents must be documented with:

- Incident timeline and chronology
- Technical details and evidence
- Impact assessment and affected parties
- Response actions taken
- Communication records
- Lessons learned and improvements

8.2 Record Retention

- **Incident Reports:** 7 years minimum
- **Investigation Evidence:** 7 years or until legal matters resolved
- **Communication Records:** 7 years
- **Training Records:** 3 years

---

9. POST-INCIDENT ACTIVITIES

9.1 Post-Incident Review (Within 5 business days)

Conduct comprehensive review including:

- Root cause analysis
- Response effectiveness evaluation
- Communication assessment
- Process improvement opportunities
- Training needs identification

9.2 Remediation Actions

- Implement security improvements
- Update policies and procedures
- Conduct additional staff training
- Enhance monitoring capabilities

- Review vendor security practices

9.3 Lessons Learned Documentation

- What worked well in the response
- What could be improved
- Specific action items with owners and deadlines
- Updates to incident response procedures

---

10. TRAINING AND TESTING

10.1 Staff Training

- **All Employees:** Annual security awareness training
- **Response Team:** Quarterly incident response training
- **New Hires:** Security training within first week

10.2 Incident Response Testing

- **Tabletop Exercises:** Quarterly scenario-based discussions
- **Simulation Exercises:** Semi-annual simulated incidents
- **Full Drills:** Annual end-to-end incident response test

10.3 Plan Maintenance

- Review and update policy annually
- Update contact information quarterly
- Revise procedures based on lessons learned
- Validate technical procedures with system changes

---

11. POLICY COMPLIANCE

11.1 Mandatory Reporting

All security incidents, regardless of severity, must be reported to the security team. Failure to report known incidents may result in disciplinary action.

11.2 Regular Reviews

This policy is reviewed annually or following any major incident. All team members are responsible for understanding and following these procedures.

11.3 Policy Updates

Updates to this policy are communicated to all staff within 30 days of approval.

Document Control:

- **Created:** August 29, 2025
- **Last Reviewed:** September 1st, 2025
- **Next Review:** September 2026
- **Approved By:** Markus Kellermann, CEO

Contact Information:

- **Policy Owner:** markus@itsconvo.com

This policy should be reviewed by qualified security and legal professionals. Regular testing and updates are essential for maintaining effective incident response capabilities.