Incident Response Card

Emergency Contact Reference | Free Download

Keep this card accessible at all times. In the event of a cybersecurity incident—ransomware, data breach, business email compromise, unauthorized access, or any suspected security event—use this card to guide your immediate response and contact the right people fast. Speed is critical: most cyber insurance policies require notification within 24–72 hours of discovering an incident.

STOP. BEFORE ANYTHING ELSE: Do not attempt to investigate, clean, or fix the problem yourself. Do not turn off affected systems unless directed by your IT team or incident response provider. Do not communicate about the incident on potentially compromised systems (email, Slack, Teams). Use phone calls or out-of-band communication only.

Organization Information

Organization Name:		**Policy #:**	
Prepared By:		**Date:**	
Location(s):		**Version:**	

Immediate Response Actions (First 30 Minutes)

Follow these steps in order. Do not skip steps. Document everything.

1. **DETECT & CONFIRM**
   Verify the incident is real. Note what you observed: error messages, unusual behavior, ransom notes, unauthorized access, data loss, or suspicious emails. Record the exact time of discovery.

2. **CONTAIN & ISOLATE**
   Disconnect affected devices from the network (unplug Ethernet, disable Wi-Fi). Do NOT power off. Isolate affected servers or workstations. Block compromised accounts. Preserve evidence.

3. **CALL YOUR INCIDENT RESPONSE TEAM**
   Contact your IT department, managed service provider, or incident response retainer immediately. Use the Emergency Contact Table on Page 2. Use phone calls—not email.

4. **NOTIFY MANAGEMENT & LEGAL**
   Alert executive leadership and legal counsel. They will determine regulatory notification obligations and authorize the incident response budget.

5. **CONTACT YOUR INSURANCE BROKER**
   Call First Underwriters at **(425) 242-5357** or your designated broker. Your cyber policy likely requires prompt notification. Your carrier may have a breach response hotline and pre-approved vendors.

6. **DOCUMENT EVERYTHING**
   Start an incident log immediately. Record times, actions taken, people contacted, and observations. Take photos of screens. This documentation is critical for insurance claims and legal proceedings.

Emergency Contact Directory

Complete this table and distribute to all key personnel. Store physical copies in a secure location separate from your IT systems—if your network is compromised, digital-only copies may be inaccessible.

Role / Function	Name	Phone (24/7)	Priority
IT Department / Help Desk			**Call First**
Managed Service Provider (MSP)			**Call First**
Incident Response Provider / Retainer			**Call First**
CEO / President / Business Owner			**Within 30 min**
CFO / Controller			**Within 1 hour**
Legal Counsel (Internal)			**Within 1 hour**
Legal Counsel (External / Breach)			**Within 1 hour**
Insurance Broker — First Underwriters	(425) 242-5357	(425) 242-5357	**Within 1 hour**
Cyber Insurance Carrier Hotline			**Within 24 hrs**
HR Director / Manager			**Within 2 hours**
Communications / PR Lead			**Within 2 hours**
Forensic Investigation Firm			**As directed**
FBI / IC3 (Federal)		ic3.gov	**As required**
Local Law Enforcement			**As required**

Pre-Approved Vendor Quick Reference

Many cyber insurance policies include pre-approved vendors for breach response services. Using non-approved vendors may affect coverage. Check your policy or call your broker before engaging vendors.

Service	Vendor Name	Phone / Contact	Policy Approved?
Digital Forensics & IR			[ ] Yes [ ] No
Breach Notification / Mailing			[ ] Yes [ ] No
Credit Monitoring Provider			[ ] Yes [ ] No
Public Relations / Crisis Comms			[ ] Yes [ ] No
Breach Coach / Attorney			[ ] Yes [ ] No
Ransom Negotiation Firm			[ ] Yes [ ] No
Data Recovery Specialist			[ ] Yes [ ] No

Incident Severity Classification

Quickly classify the incident to determine the appropriate response level and notification timeline.

	Severity	Examples	Response Time	Insurer Notice
🔴	**CRITICAL**	Active ransomware, confirmed data breach with PII/PHI exposure, business email compromise with funds transferred, active threat actor in network	**Immediate (within 15 min)**	Within 24 hours
🟠	**HIGH**	Suspected data exfiltration, compromised admin credentials, malware on multiple systems, unauthorized access to sensitive data	**Within 30 min**	Within 48 hours
🟡	**MEDIUM**	Single system malware infection, phishing email with credentials entered, unauthorized access attempt detected and blocked, suspicious login activity	**Within 2 hours**	Within 72 hours
🟢	**LOW**	Phishing email reported (no click), single failed login attempts, minor policy violation, suspicious but unconfirmed activity	**Within 24 hours**	Monitor only

Response Timeline: First 72 Hours

Use this timeline to track progress through the critical first 72 hours of incident response.

Timeframe	Action Items	Responsible	Completed
0 – 15 min	Detect, confirm, and contain the incident. Isolate affected systems.	First Responder	[ ] ___:___
15 – 30 min	Notify IT / MSP / IR provider. Begin incident documentation log.	First Responder	[ ] ___:___
30 – 60 min	Notify executive leadership and legal counsel. Assess severity level.	IT Lead	[ ] ___:___
1 – 4 hours	Contact insurance broker. Engage pre-approved forensic and legal vendors.	Management	[ ] ___:___
4 – 12 hours	Begin forensic investigation. Preserve evidence and system images.	IR Team	[ ] ___:___
12 – 24 hours	Assess data exposure. Identify affected individuals and records.	IR Team / Legal	[ ] ___:___
24 – 48 hours	Determine regulatory notification obligations. Draft breach notifications.	Legal / Comms	[ ] ___:___
48 – 72 hours	Submit insurance claim. Begin remediation and recovery. Notify regulators if required.	Management	[ ] ___:___

Incident Type Quick Reference

Identify the type of incident to determine the appropriate specialized response actions.

Incident Type	Indicators	Immediate Actions
Ransomware	Files encrypted, ransom note displayed, file extensions changed, systems inaccessible	Isolate ALL affected systems immediately. Do NOT pay ransom without consulting legal and insurer. Preserve encrypted files. Contact IR team and insurance broker.
Data Breach / Exfiltration	Unusual data transfers, large outbound traffic, unauthorized cloud access, sensitive files accessed	Block exfiltration path. Identify scope of exposed data (PII, PHI, financial). Preserve access logs. Engage forensics and breach counsel immediately.
Business Email Compromise (BEC)	Executive impersonation, wire transfer requests, vendor payment redirect, invoice fraud	Contact bank IMMEDIATELY to recall wire. Freeze affected accounts. Preserve the fraudulent email (headers and all). File IC3 report. Notify insurer.
Phishing / Credential Theft	Employee clicked malicious link, entered credentials on fake site, credential harvesting confirmed	Reset compromised passwords immediately. Force MFA re-enrollment. Scan for lateral movement. Check for email forwarding rules. Review recent login activity.
Malware / Virus	Antivirus alerts, unusual system behavior, unauthorized processes, performance degradation	Isolate infected device. Run full EDR scan. Check other devices on same network segment. Preserve malware sample if possible for forensic analysis.
Insider Threat	Unauthorized data access by employee, sabotage, policy violations, unusual after-hours activity	Restrict account access immediately. Preserve audit logs and access records. Engage HR and legal. Do not alert the individual until directed by legal.
Denial of Service (DDoS)	Website/services unavailable, massive traffic spike, customer-facing systems offline	Activate DDoS mitigation (CDN/ISP). Document the attack pattern. Redirect traffic if possible. Notify affected customers. Contact ISP for upstream filtering.

Regulatory Notification Requirements

Data breach notification laws vary by state and type of data. This is a general reference—always consult your breach counsel for specific obligations.

Regulation / Law	Applies When	Notification Deadline	Notify
Washington State (RCW 19.255)	WA residents' PII breached	Within 30 days of discovery	Affected individuals + WA AG (>500)
HIPAA (Healthcare)	PHI of patients compromised	Within 60 days	HHS + individuals + media (>500)
PCI DSS (Payment Cards)	Cardholder data compromised	Immediately upon discovery	Card brands + acquiring bank
SEC (Public Companies)	Material cybersecurity incident	Within 4 business days	SEC Form 8-K filing
GDPR (EU Data)	EU resident data breached	Within 72 hours	Supervisory authority + individuals
State AG (General)	Varies by state	Varies (30–90 days typical)	State Attorney General

Incident Documentation Log

Use this log to record all incident activity in real time. Attach additional sheets as needed. This documentation is critical for forensic investigation, insurance claims, legal proceedings, and regulatory compliance.

Date	Time	Action / Observation	Person	Status
		Incident discovered / reported		

Cyber Insurance Claim Checklist

When filing a cyber insurance claim, your carrier will typically require the following documentation. Begin collecting these items as early as possible during the incident.

	Required Documentation	Notes / Status
☐	Completed incident report with timeline of events	
☐	Incident documentation log (page 5 of this card)	
☐	Forensic investigation report from approved vendor	
☐	Evidence of when the incident was discovered and when the carrier was notified	
☐	List of affected systems, data types, and number of records exposed	
☐	Evidence of security controls in place at time of incident (MFA, EDR, backups)	
☐	Copy of breach notification letters sent to affected individuals	
☐	Proof of regulatory notifications filed (state AG, HHS, SEC, etc.)	
☐	Financial loss documentation (business interruption, ransom payment, legal fees)	
☐	Communication records with law enforcement (if applicable)	
☐	Evidence of remediation actions taken to prevent recurrence	
☐	Quotes or invoices from breach response vendors (forensics, legal, notification, credit monitoring)	

IMPORTANT: Most cyber insurance policies have strict notification requirements. Failure to notify your carrier within the required timeframe (typically 24–72 hours) may jeopardize your coverage. When in doubt, call your broker at First Underwriters: **(425) 242-5357**.

Print & Post: Quick Response Reference Card

Cut along the border and post this card in server rooms, IT offices, and break rooms. Distribute to all employees with access to sensitive systems.

CYBER INCIDENT? DO THIS NOW.

1. **STOP. Do not attempt to fix the problem yourself.**
2. DISCONNECT affected devices from the network (unplug cable / disable Wi-Fi).
3. DO NOT power off computers. Leave them running for forensics.
4. **CALL IT immediately:** _____
5. **CALL your manager:** _____
6. **CALL insurance broker: (425) 242-5357 — First Underwriters**
7. DOCUMENT what you saw: time, screens, error messages. Take photos.
8. DO NOT communicate about the incident using email or company chat.
9. USE phone calls only until IT confirms systems are safe.

DO NOT: Pay ransom | Click suspicious links | Delete files | Restart computers

Card Distribution Record

Track where physical copies of this card have been posted or distributed.

Location / Recipient	Date Posted	Posted By

Disclaimer

This Incident Response Card is provided by First Underwriters Insurance Brokers as a complimentary resource for informational and risk management purposes only. It does not constitute legal, technical, or professional advice. Every organization's regulatory environment, technology infrastructure, and insurance policy terms are unique. This card should be customized to reflect your specific circumstances and reviewed by legal counsel, IT leadership, and your insurance broker. Regulatory notification timelines are subject to change; always verify current requirements. Completion does not guarantee insurance coverage or claim approval.

First Underwriters Insurance Brokers

4055 Lake Washington Blvd NE, Suite 100, Kirkland, WA 98033 | (425) 242-5357 | firstunderwriters.com