

Cyber incident role card

For management, IT and business teams: assign responsibilities, communicate securely and record decisions. Add contacts and decision authority before use. For an urgent suspicion, call the agreed IT contact immediately; do not wait for complete paperwork.

Organization: _____ Owner: _____
Reviewed on: _____ Approved by: _____

Role and task	Name and backup	Phone, time zone and fallback
Incident lead Coordinate priorities, actions and situation updates	_____ _____	_____ _____
IT or IT provider Assess scope, lead containment and recovery	_____ _____	_____ _____
Management and business owner Assess operational impact and authorize decisions	_____ _____	_____ _____
Communications Issue approved internal and external updates	_____ _____	_____ _____
Privacy and legal Assess notification duties and external involvement	_____ _____	_____ _____

Communication and decision authority

Approved fallback if email may be compromised: _____
Who may isolate or shut down systems: _____
Who approves recovery and external messages: _____
Next situation update and responsible person: _____

Small teams may combine roles, but each responsibility and deputy should remain explicit. Agree how to reach people outside normal hours. Do not rely on potentially compromised communication channels without checking them.

Initial internal report

For the reporting person and incident lead. Record observations, label assumptions and leave unknowns explicit. This is an internal report; it does not replace any required external notification.

Field	Entry
Case ID and reporting person Safe callback contact	
Discovery date and time Include time zone	
Observation and source What is actually known	
Affected services and business impact What no longer works	
Actions already taken Who did what and when	
Contacts informed and handover Who is handling the report	
Open questions and next update Owner and time	

Hand over information securely

Do not record passwords, MFA codes or unnecessary personal data. Reference evidence using internal IDs and approved storage locations. Have qualified staff preserve originals and logs; agree retention and access rights. Do not open suspicious files to inspect them or forward them through unapproved channels.

Incident log and handover

For the record keeper. Include date, time and time zone in every entry. Distinguish observations, decisions and outcomes. Copy log pages as needed and record corrections as new entries.

Case ID: _____ Record keeper: _____

Time and source	Observation or decision	Action and owner	Outcome or evidence ID
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Handover and recovery

Current scope and remaining risks: _____
Open actions with owners and due dates: _____
Handed over by / to / time: _____
Recovery approved by / time / conditions: _____
Functional checks, monitoring period and next review: _____

Follow up

Improvement to implement: _____
Owner / due date / effectiveness reviewed on: _____

Use and supporting guidance

Original Paragamix GmbH templates. Free to use internally, adapt and share with clients; a source link is welcome. Have responsible staff review before use. An organizational aid, not a technical response manual. Store completed records securely.

[NIST SP 800 61 Rev 3](#) | [Current version and tools](#)

United States incident contacts

Prepare these contacts before an incident. Use verified details from your contracts and policy; confirm who can authorize specialist support. In an active incident, reach your IT contact promptly without waiting to complete this page.

Role	Contact and backup	Phone, hours and time zone
Forensics / DFIR		
Cyber insurer / claims		
Legal / breach counsel		

Policy or engagement reference:

Official reporting contacts

Ransomware or extortion: contact your local [FBI Field Office](#) and report to [IC3](#). These reporting routes do not replace your technical response team.

CISA Operations Center: +1 844 729 2472, available 24/7. A report does not guarantee individual technical assistance. [Official contact source](#)

Notification review and decisions

Have counsel assess the affected information, states of residence, industry and contracts. There is no universal 72-hour U.S. deadline. Review HIPAA, SEC or financial-sector rules where applicable and confirm current CIRCIA requirements if relevant. Ransom payments may violate U.S. sanctions; involve counsel, your insurer and law enforcement.

Review owner and safe contact:

Affected states or jurisdictions:

Decision, rationale and next review time:

Keep evidence references and approvals in the incident log, including the time zone. To record and export your incident online, use the [IT Emergency Navigator](#).

Guidance: [FTC response guide](#) | [OFAC ransomware advisory](#) | [NIST SP 800-61 Rev. 3](#)

Sources checked Sep 14, 2026. Confirm current requirements with the responsible specialists. U.S. focus does not exclude additional obligations for international operations.