

Contacts and communication

Worksheet 1 of 5. U.S. edition. Complete these fields with management, IT and operations. Keep a current copy in an agreed offline location.

Organization / site: _____ Owner: _____
Version / next review: _____ Approved by: _____

Who takes responsibility

Role	Name and backup	Verified phone, time zone and fallback
Coordination / lead	_____ _____	_____ _____
IT / IT provider	_____ _____	_____ _____
Operations / continuity	_____ _____	_____ _____
Facilities / safety	_____ _____	_____ _____

If email or phones fail

Approved fallback channel: _____
If that also fails, agreed meeting point: _____
Offline location of this pack and authorized users: _____
Last contact test / result: _____

Report and coordinate

For immediate danger, follow site safety and evacuation procedures and contact local emergency services when needed. Otherwise report what you observed, when, where and which activity is affected. Obtain acknowledgement; use the agreed deputy if no one responds. Do not improvise interventions on electrical or safety-critical systems.

Do not record passwords or recovery keys. Restrict distribution of personal contact details. Do not publish completed worksheets publicly.

Critical activities and continuity

Worksheet 2 of 5. U.S. edition. Copy this sheet for each important activity. Timing estimates are planning assumptions to be agreed and checked with the responsible people.

Planning question	Your organization's agreement
Activity and responsible person	
Impact on customers, people and operations	
When does disruption become unacceptable and why	
People, IT, data, premises and providers needed	
Minimum service and approved fallback process	
Who activates fallback operations and when they end	
Recovery target and conditions for authorization	

Agree before resuming normal operations

Who confirms safety and availability? How will the service be tested? How will paper records and backlogs be reconciled without duplicate or missing transactions?

Having a backup does not establish that recovery will work. IT and operations should separately check data requirements, dependencies and tested recovery options.

A 30 minute team exercise

Worksheet 3 of 5. U.S. edition. A discussion exercise using fictional information. Do not shut down systems, trigger real alerts or use customer data. A real incident ends the exercise.

Date: _____ Facilitator: _____ Recorder: _____

Participants / roles: _____

Time	Inject and questions
0–5 min	Agree the aim: test contact arrangements and one critical activity. Assign roles and confirm exercise rules.
5–15 min	9:10 a.m. Central Time: Site power fails. ERP and office phones are unavailable. The cause is unknown. Who checks safety? Who coordinates? How does the team reach the deputy without email?
15–25 min	9:30 a.m. Central Time: There is no reliable recovery estimate; mobile connections are unreliable. An important customer order is due. Which fallback process is authorized? What is paused? Who communicates with whom, and how?
25–30 min	Capture the three most important gaps. Assign an owner, a deadline and observable completion evidence to each.

Record observations

Question / decision	Observation or unresolved gap
_____	_____ _____
_____	_____ _____

To rehearse coordination, open the IT Emergency Navigator with fictional information. Select United States and America/Chicago. Do not call contacts or submit agency reports during the exercise.

[IT Emergency Navigator](#)

Actions and next review

Worksheet 4 of 5. U.S. edition. Close the exercise by recording results and assigning the next steps. Follow up to verify that the actions are implemented.

Gap and action	Owner / deadline	Evidence / status

Action follow-up date:
Who checks completion:
Next exercise and focus:

Keep the pack current

Review contacts, fallback channels and activities after changes and incidents, and agree a regular internal review date. Replace outdated offline copies. Mark an action complete only with evidence, such as a recorded contact test.

Use and sources

These original Paragamix GmbH templates may be used internally, adapted and shared with clients free of charge. A source link is welcome but not required. External materials retain their own terms.

[NIST SP 800-61 Rev. 3](#) | [CISA tabletop exercise materials](#)

Current version and sources

These worksheets support preparation. They are not a complete continuity plan or a compliance certificate. Have the responsible teams review and approve them before operational use.

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.