Incident Response and Preparedness Template

To handle incidents, organizations follow incident response playbooks containing policies and procedures for each step of response. These playbooks also cover incident preparation and prevention, including cybersecurity training and auditing.

Consider using this template as part of your incident response playbook. With this template, you can document your incident response and prepare for future incidents. You can also edit each section to fit the needs of your organization. Note that your organization may have additional forms or reports that you must complete. Also note that your organization’s incident response playbook should indicate the person responsible for updating and maintaining incident documentation.

# Incident Response Teams and Responsibilities

In the Team column, list the person to contact on each team if an incident occurs. This person ensures that the team fulfills its responsibilities toward the incident. Examples of team responsibilities are listed in this table.

|  |  |
| --- | --- |
| Team | Responsibilities |
| Management | Compliance |
| Contact name:  Phone:  Email: | Ensures that all members are aware of the organization’s security policies |
| Confirms that all incident response team members know whom to contact if an incident occurs |
| Verifies that all incident responders have access to journals and access to incident response toolkits to complete all parts of the response |
| Ensures that all members regularly participate in drills to practice the incident response process and improve proficiency |
| Information Assurance | Compliance |
| Contact name:  Phone:  Email: | Receives information about a breach according to timeline and format mandated by regulatory requirements |
| IT Support |  |
| Contact name:  Phone:  Email: | Manages access to systems and applications for internal staff and partners |
| Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyberattack |
| Legal | Compliance |
| Contact name:  Phone:  Email: | Confirms requirements for informing employees, customers, and the public about cyberbreaches |
| Checks in with local law enforcement |
| Ensures the IT team has legal authority for privilege account monitoring |
| Public Affairs and Media Relations | Communication |
| Contact name:  Phone:  Email: | Communicates externally with customers, partners, and the media |
| Coordinates all communications and requests for interviews with internal subject matter experts and the security team |
| Keeps and updates customizable drafts of incident communications plans and statements for use if an incident occurs |
| Human Resources | Compliance |
| Contact name:  Phone:  Email: | Coordinates internal employee communications regarding breaches of personal information and responds to questions from employees |
| Business Continuity Planning | Communication |
| Contact name:  Phone:  Email: | Communicates externally with customers, partners, and the media |
| Coordinates all communications and requests for interviews with internal subject matter experts and the security team |
| Keeps and updates customizable drafts of incident communications guidelines and statements for use in case an incident occurs |
| Physical Security and Facilities Management | Security |
| Contact name:  Phone:  Email: | Manages user privileges, enterprise password protection, and role-based access control |
| Discovers, audits, and reports on all privilege usage |
| Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are |
| Monitors use of privileged accounts and proactively searches for signs of compromise |
| Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks |
| Takes action to prevent the spread of a breach by updating privileges |

# Incident Location and Type

Indicate the incident’s location and type, and make multiple selections if appropriate. If the choices listed do not accurately represent the location or type of incident, select “Other” and describe the location or type.

|  |  |
| --- | --- |
| Location of Incident | Type of Incident |
| £ Management  £ Information Assurance  £ IT support  £ Legal  £ Public Affairs  £ HR  £ Other: | £ External/removable Data  £ Attrition  £ Web  £ Email  £ Impersonation  £ Loss or theft of equipment  £ Other: |

# Incident Response Checklist

Use this checklist to track completion of steps in each phase of the response.

|  |  |  |  |
| --- | --- | --- | --- |
| Phase | Action | Team or Team Member(s) | Day/Time of Action |
| Detection and Analysis | Describe how the incident was discovered, including where it occurred and who reported it. |  |  |
| Determine the incident’s scope, including its impacts on security and business. |  |  |
| Report the incident to all appropriate parties. |  |  |
| Containment | Isolate the problem if possible. |  |  |
| Change all passwords. |  |  |
| Protect evidence and backup compromised systems. |  |  |
| Create forensic copies of evidence. |  |  |
| Notify employees about breach containment. |  |  |
| Eradication | Determine if eradication is possible. |  |  |
| Find and address all exploited vulnerabilities. |  |  |
| Close firewall ports and connections. |  |  |
| Remove malware and other artifacts of the attack. |  |  |
| Test devices for removal of malware. |  |  |
| Recovery | Patch and harden affected systems. |  |  |
| Close network access. |  |  |
| Return affected systems to an operational state. |  |  |
| Test affected systems for normal functioning. |  |  |
| Notify employees about recovery. |  |  |
| Begin additional monitoring if needed. |  |  |
| Post-Incident Activity | Ensure all incident documentation is complete. |  |  |
| Hold a lessons learned meeting. |  |  |
| Create an incident response report. |  |  |
| Review forensic evidence. |  |  |
| Update the incident response playbook if needed. |  |  |
| Hold training sessions. |  |  |

# Additional Resources

For more guidance, consult the following resources:

* [Computer Security Incident Handling Guide](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf) – a NIST document that examines each phase of incident response in detail
* [Incident Handler’s Handbook](https://www.sans.org/white-papers/33901/) – a SANS document that provides helpful guidance on incident response, including an incident response checklist
* [Cynet’s Incident Response Template](https://cdt.ca.gov/wp-content/uploads/2017/03/templates_incident_response_plan.doc) – another helpful incident response template worth consulting as you develop your organization’s incident response plan