

# Incident Response Plan (IRP) Template

**1. Introduction**

**1.1 Purpose of the Plan**

This Incident Response Plan (IRP) is designed to outline the procedures to follow when a cybersecurity incident occurs. It aims to ensure that incidents are identified, contained, analyzed, and resolved promptly while minimizing damage to the organization’s assets, reputation, and operations.

**1.2 Scope**

This plan applies to all employees, systems, applications, and data within the organization and covers all types of cybersecurity incidents, including data breaches, system compromises, malware attacks, and unauthorized access.

**1.3 Definitions**

* **Incident:** Any event that threatens the confidentiality, integrity, or availability of the organization’s data, systems, or networks.
* **Critical Incident:** A major event that disrupts or has the potential to disrupt business operations significantly, such as a data breach, ransomware attack, or system compromise.

**2. Incident Response Team (IRT)**

**2.1 Incident Response Team Roles and Responsibilities**

* **Incident Response Manager (IRM):**
	+ Overall leader of the incident response process.
	+ Ensures all necessary resources are allocated.
	+ Coordinates with external stakeholders, including law enforcement, if necessary.
* **IT Security Specialist:**
	+ Technical lead on identifying and containing the threat.
	+ Performs forensic analysis of affected systems.
	+ Works with other departments to secure and restore systems.
* **Legal & Compliance Officer:**
	+ Ensures legal compliance throughout the incident response.
	+ Coordinates with regulatory bodies and assists with breach notification requirements.
	+ Advises on risk mitigation and liability management.
* **Communications Officer:**
	+ Responsible for internal and external communication during the incident.
	+ Coordinates messaging for customers, vendors, and the media if needed.
	+ Ensures a consistent and clear flow of information.
* **HR and Employee Relations:**
	+ Ensures that internal employees are informed and manages employee-related aspects of the incident.
	+ Helps address internal or external threats involving employees (e.g., insider threats).
* **Third-Party Experts (if applicable):**
	+ External cybersecurity experts or consultants brought in for specialized expertise or incident handling.

**2.2 Contact Information**

Provide the names, titles, phone numbers, and email addresses of key IRT members.

| **Name** | **Role** | **Phone** | **Email** |
| --- | --- | --- | --- |
| John Doe | Incident Response Manager | (555) 123-4567 | jdoe@company.com |
| Jane Smith | IT Security Specialist | (555) 234-5678 | jsmith@company.com |
| Michael Brown | Legal & Compliance Officer | (555) 345-6789 | mbrown@company.com |
| Emily White | Communications Officer | (555) 456-7890 | ewhite@company.com |
| Sarah Green | HR & Employee Relations | (555) 567-8901 | sgreen@company.com |

**3. Incident Detection & Identification**

**3.1 Incident Detection Methods**

* **Network Monitoring Tools:** Regular scanning for unusual activity (e.g., firewalls, IDS/IPS).
* **Endpoint Security Software:** Detects malware, ransomware, or unauthorized access.
* **User Reports:** Employees reporting suspicious activities (e.g., phishing attempts, strange emails).
* **Third-Party Alerts:** Notifications from external vendors or partners regarding vulnerabilities or threats.

**3.2 Incident Classification**

* **Minor Incident:** Does not significantly affect business operations; can be contained and resolved quickly.
* **Moderate Incident:** Affects certain systems or data but can be mitigated without major business disruptions.
* **Critical Incident:** Major disruption to operations, involves sensitive data breach, system compromise, or significant downtime.

**3.3 Initial Incident Assessment**

* Verify the incident and assess its scope.
* Classify the incident based on severity.
* Identify affected systems and determine potential business impacts.

**4. Incident Containment**

**4.1 Short-Term Containment**

* **Disconnect:** If the incident involves a compromised system, isolate affected systems to prevent further damage (e.g., disconnect from the network).
* **Apply Temporary Measures:** Block malicious IP addresses, disable compromised accounts, and disable external access if needed.

**4.2 Long-Term Containment**

* **Implement Network Segmentation:** If necessary, segment affected network areas to contain the spread of the attack.
* **Access Control Changes:** Change passwords, revoke compromised user accounts, and apply tighter access controls.

**4.3 Eradication**

* **Malware Removal:** Clean affected systems of malicious software or backdoors.
* **Restore Systems:** After containment, restore systems from clean backups or from known good states.

**5. Incident Analysis and Investigation**

**5.1 Forensic Investigation**

* Gather evidence of the attack (e.g., logs, network traffic, malware samples).
* Work with external forensic experts if needed to trace the incident’s origin and impact.
* Identify affected data, systems, and people.
* Determine whether the attack was targeted or opportunistic.

**5.2 Root Cause Analysis**

* Identify the cause of the incident (e.g., phishing, vulnerability exploitation, insider threat).
* Assess if the incident resulted from an existing vulnerability or if it was the result of a failure in internal security controls.

**6. Communication & Reporting**

**6.1 Internal Communication**

* **Employees:** Notify employees about the incident (without causing panic) and advise on next steps, including reporting suspicious activities.
* **Management:** Keep senior leadership informed about the progress of containment, investigation, and recovery efforts.

**6.2 External Communication**

* **Customers/Clients:** Notify affected customers or clients if their data has been compromised. Include details of the incident, steps taken, and what they can do to protect themselves.
* **Regulatory Bodies:** Notify regulatory authorities (e.g., SEC, FTC) as required by laws like GDPR, HIPAA, or CCPA if personal data is involved.
* **Media:** Prepare an official statement if the incident has public implications, ensuring all communication is consistent and accurate.

**7. Recovery**

**7.1 System Restoration**

* Begin the process of restoring systems, networks, and data from secure backups.
* Test systems before reintroducing them to the network to ensure they are free of malicious activity.

**7.2 Business Continuity**

* Activate Business Continuity Plans (BCPs) to ensure essential services continue.
* Restore critical systems based on their priority to minimize operational downtime.

**7.3 Post-Incident Review**

* Conduct a debrief meeting with the Incident Response Team and key stakeholders.
* Identify lessons learned and areas of improvement.
* Review and update internal controls to prevent similar incidents.

**8. Post-Incident Activities**

**8.1 Root Cause Analysis Report**

* Prepare a detailed report that includes:
	+ Timeline of events
	+ Description of the attack
	+ Evidence collected
	+ Impact assessment
	+ Recovery actions taken

**8.2 Improvement Plan**

* Based on the lessons learned, update the Incident Response Plan, cybersecurity policies, and employee training programs.
* Implement new or improved safeguards, tools, and procedures to prevent recurrence.

**8.3 Legal and Compliance Considerations**

* Ensure that all legal reporting requirements (e.g., data breach notifications) have been met.
* Work with legal counsel to handle any litigation, regulatory fines, or penalties.

**9. Training and Awareness**

**9.1 Employee Training**

* Regularly train employees on how to identify and report incidents.
* Conduct phishing and social engineering tests to raise awareness.

**9.2 Simulation Exercises**

* Run periodic incident response drills (tabletop exercises) to practice the execution of this plan.
* Review the outcomes and improve the process based on feedback.

**10. Incident Response Plan Review**

**10.1 Plan Review and Updates**

* Review and update the Incident Response Plan annually or after significant incidents.
* Ensure that all contact information, roles, and procedures are up-to-date.
* Test and improve the plan regularly through simulations.

**11. Appendix**

* **Incident Response Checklist:** A detailed checklist of actions to be taken during each phase of the incident response.
* **Communication Templates:** Pre-written templates for communicating with employees, customers, and regulatory bodies during an incident.
* **Incident Report Form:** A standardized form to document all incident details, responses, and actions taken.

This **Incident Response Plan Template** is designed to be a flexible document that can be adapted to your organization's needs. Regular reviews, updates, and testing of this plan will help your business stay prepared for cybersecurity threats and minimize potential damage during incidents.

**Incident Response Checklist**

**1. Preparation**

* **Ensure Incident Response Team (IRT) is established**:
	+ Confirm roles and contact information for key personnel.
	+ Ensure team members are trained and familiar with their responsibilities.
* **Maintain up-to-date incident response tools**:
	+ Ensure monitoring, logging, and detection tools are operational.
	+ Verify that backups are regularly scheduled and intact.
* **Ensure all communication channels are secured**:
	+ Confirm secure communication platforms are in place for the IRT (e.g., encrypted email, secure messaging systems).

**2. Detection & Identification**

* **Identify the incident**:
	+ Review alerts from network monitoring tools, antivirus software, firewalls, or employee reports.
	+ Confirm if this is an actual security incident or a false alarm.
* **Classify the incident**:
	+ Minor: Low impact, contained with minimal disruption.
	+ Moderate: Affects operations but can be managed with minimal downtime.
	+ Critical: Major system compromise, significant operational disruption, or data breach.
* **Document incident details**:
	+ Record the time and date of discovery.
	+ Capture initial evidence (e.g., logs, screenshots, system states).

**3. Containment**

**3.1 Short-Term Containment**

* **Isolate affected systems**:
	+ Disconnect compromised systems from the network or restrict access (if possible).
	+ Disable affected user accounts or services.
* **Block malicious traffic**:
	+ Block IP addresses or domains associated with the attack.
	+ Stop or mitigate any active malicious processes (e.g., malware running).
* **Preserve evidence**:
	+ Ensure logs and other key evidence are saved and protected for forensic analysis.

**3.2 Long-Term Containment**

* **Limit further access**:
	+ Restrict access to critical systems to authorized personnel only.
	+ Apply additional security controls if needed (e.g., network segmentation, enhanced monitoring).
* **Implement temporary security measures**:
	+ Apply patches or disable vulnerable services that were exploited in the attack.
	+ Deploy firewalls or endpoint protection tools to limit further damage.

**4. Eradication**

* **Remove malware or unauthorized access**:
	+ Scan and remove any malware or backdoors left by the attacker.
	+ Identify and delete malicious files, processes, or registry entries.
* **Fix vulnerabilities**:
	+ Apply security patches to any exploited vulnerabilities.
	+ Change passwords, especially for privileged accounts.
* **Check for persistence mechanisms**:
	+ Investigate whether the attacker has set up any mechanisms for regaining access (e.g., backdoors, scheduled tasks).
	+ Ensure all such persistence mechanisms are identified and removed.

**5. Recovery**

* **Restore systems from backups**:
	+ Restore affected systems using clean backups (ensure the backups are malware-free).
	+ Validate the integrity of the data and systems after restoration.
* **Reintegrate systems into the network**:
	+ Gradually reintroduce systems to the network once confirmed that they are secure.
	+ Monitor restored systems closely for signs of recurring incidents.
* **Monitor the network and systems for signs of further issues**:
	+ Increase monitoring for abnormal activity or indicators of compromise (IoC).
	+ Check for signs of lateral movement or additional malware.

**6. Communication**

**6.1 Internal Communication**

* **Notify the Incident Response Team (IRT)**:
	+ Send out immediate notifications to IRT members to start the response process.
* **Alert senior management**:
	+ Inform leadership about the incident, potential impact, and ongoing response efforts.
* **Update employees**:
	+ Communicate to employees about any disruptions or actions they need to take (e.g., changing passwords, avoiding phishing emails).
	+ Provide guidance on any actions employees should take to ensure their devices are secure.

**6.2 External Communication**

* **Notify customers, partners, and vendors if affected**:
	+ Send out notifications to affected stakeholders about the incident, including any potential data breaches.
	+ Provide guidance on steps customers need to take (e.g., monitoring accounts, resetting passwords).
* **Notify regulatory bodies if required**:
	+ Report the incident to regulatory authorities (e.g., GDPR, CCPA, HIPAA) within the required timelines if personal data was compromised.
* **Prepare external communication statements**:
	+ Draft and review a public statement if the incident is severe enough to require media communication.

**7. Documentation**

* **Document all actions taken**:
	+ Record the timeline of events and actions taken during the response.
	+ Collect and securely store all evidence (e.g., logs, screenshots, email correspondence).
* **Prepare an Incident Report**:
	+ Develop a detailed post-incident report, including the nature of the attack, timeline of actions taken, recovery steps, and root cause analysis.
	+ Include recommendations for improving security based on the lessons learned.
* **Update incident response procedures if needed**:
	+ Review the effectiveness of the incident response process and make necessary improvements.

**8. Post-Incident Activities**

* **Conduct a post-incident review (Lessons Learned)**:
	+ Gather the Incident Response Team and key stakeholders to review the incident.
	+ Discuss what went well, what could be improved, and how to strengthen the organization’s defenses.
* **Identify gaps in security**:
	+ Review the attack vector and identify any weaknesses or vulnerabilities that need to be addressed.
	+ Update security protocols, policies, and defenses based on the findings.
* **Implement preventive measures**:
	+ Improve training, awareness programs, and incident detection methods to avoid future incidents.
	+ Apply additional security measures or tools (e.g., stronger endpoint protection, advanced threat detection systems).
* **Verify compliance with legal requirements**:
	+ Confirm that all regulatory and compliance requirements (e.g., breach notifications, reporting) were met.
	+ Work with legal counsel to ensure proper documentation and adherence to regulations.
* **Conduct training and awareness**:
	+ Train employees on new or updated security protocols and policies.
	+ Run mock drills or phishing simulations to improve future response readiness.

**9. Review and Update**

* **Review and update the Incident Response Plan**:
	+ Based on lessons learned, update the IRP to address new risks or improve the process.
* **Test the updated plan**:
	+ Run tabletop exercises or simulations to ensure the new procedures work effectively.

**Notes**

* Always ensure that all sensitive data (e.g., employee or customer information) is handled according to applicable laws (e.g., GDPR, HIPAA).
* Make sure any external communications are reviewed by the Legal and Communications teams before being sent out.

**Conclusion**

This **Incident Response Checklist** is a critical tool for ensuring that your team can respond effectively to a cybersecurity incident. It helps maintain a structured approach to identifying, containing, and resolving security issues, ultimately reducing downtime and minimizing damage to the organization. Regular reviews and updates to this checklist are essential to adapt to new threats and improve overall incident response capabilities.

Here are several **communication templates** you can use during an incident response. These templates are designed to maintain clear, consistent, and professional communication with various stakeholders (employees, customers, partners, vendors, and regulatory authorities) during and after a cybersecurity incident.

**1. Internal Communication Template: Incident Notification to Employees**

**Subject: Important Security Incident Notification**

Dear [Employee Name],

We are reaching out to inform you that our organization has experienced a cybersecurity incident. At this time, our Incident Response Team is actively working to investigate and contain the situation.

**What You Need to Know:**

* The incident was detected on [date and time].
* We have isolated affected systems to minimize any impact.
* We are currently working to determine the scope and impact of the incident.

**What We Need From You:**

* Please **do not** attempt to access affected systems or devices.
* If you notice any unusual activity on your accounts or systems, report it immediately to [IT support contact] or [incident response email].
* Ensure that all security software (antivirus, endpoint protection) is active and up-to-date on your devices.

We will provide updates as the situation progresses. We appreciate your cooperation and patience during this time.

If you have any questions or concerns, please reach out to [contact person, department, or IT support].

Thank you for your attention to this matter.

Sincerely,
[Your Name]
[Your Title]
[Your Organization]

**2. External Communication Template: Incident Notification to Customers**

**Subject: Security Incident Notification - [Your Company Name]**

Dear [Customer Name],

We are writing to inform you that we have experienced a cybersecurity incident that may have affected your data. We take the security of your information seriously and want to provide you with the details of the situation and the steps we are taking to resolve it.

**What Happened:**

* On [date], we detected unusual activity within our systems, which we have since identified as a security incident.
* We immediately activated our Incident Response Plan, isolated affected systems, and began a thorough investigation.

**What You Need to Know:**

* At this time, we have no reason to believe that your sensitive personal information (e.g., financial data, login credentials) has been compromised.
* We are continuing to monitor and assess the situation.

**Actions We Are Taking:**

* We have secured our systems and are working with cybersecurity experts to prevent future incidents.
* We will notify you if any additional information comes to light that affects your account.

**What You Can Do:**

* We recommend that you monitor your accounts and change your password if you haven’t already.
* If you notice any suspicious activity, please contact us immediately.

We deeply regret any inconvenience this incident may cause and are committed to ensuring that this issue is resolved swiftly. If you have any questions, please do not hesitate to reach out to our support team at [customer support email] or [phone number].

Thank you for your understanding and continued trust.

Sincerely,
[Your Name]
[Your Title]
[Your Organization]

**3. External Communication Template: Incident Notification to Partners or Vendors**

**Subject: Security Incident Notification - [Your Company Name]**

Dear [Partner/Vendor Name],

We are writing to inform you that [Your Company Name] has experienced a cybersecurity incident that may impact certain systems or services we provide. We want to ensure you are aware of the situation and understand the steps we are taking to address it.

**Incident Details:**

* The incident was detected on [date], and we have initiated our Incident Response Plan.
* Affected systems have been isolated to prevent further impact, and we are working with cybersecurity experts to investigate and mitigate the issue.

**Impact on Partnership/Service:**

* At this time, we do not believe that this incident has affected any of our mutual projects or services.
* However, we are continuing to monitor the situation and will notify you if anything changes.

**Next Steps:**

* We are taking immediate actions to secure all systems and mitigate any risks to our operations.
* If you require further clarification or need to take specific actions on your end, we will provide additional instructions as necessary.

We greatly appreciate your patience as we work to resolve this matter. If you have any questions or concerns, please do not hesitate to reach out to us at [contact information].

Sincerely,
[Your Name]
[Your Title]
[Your Organization]

**4. Regulatory Communication Template: Incident Notification (For Data Breach)**

**Subject: Data Breach Notification - [Your Company Name]**

Dear [Regulatory Authority Name],

We are writing to inform you of a data breach that has occurred within [Your Company Name]. This notification is in compliance with [applicable regulation such as GDPR, CCPA, HIPAA] requirements.

**Breach Details:**

* On [date], we detected a cybersecurity incident involving unauthorized access to our systems.
* The breach was immediately contained, and affected systems were isolated.

**Data Involved:**

* Based on our initial investigation, the compromised data includes [type of data affected, e.g., personal data, financial records, etc.].
* We have notified affected individuals and provided guidance on monitoring their accounts and mitigating potential risks.

**Steps Taken:**

* We have taken immediate steps to secure our systems, including removing unauthorized access and enhancing our security measures.
* Affected individuals have been notified, and we are providing them with support, including credit monitoring where applicable.

**Next Steps:**

* We will continue to monitor the situation and conduct a thorough investigation.
* We are implementing additional security measures to prevent future incidents.

If you require additional information or documentation, please let us know. We are committed to complying with all regulatory requirements and ensuring the protection of personal data.

Sincerely,
[Your Name]
[Your Title]
[Your Organization]

**5. Public Communication Template: Press Release (If Applicable)**

**Subject: Press Release - [Your Company Name] Cybersecurity Incident**

**FOR IMMEDIATE RELEASE**

[Your Company Name] Announces Cybersecurity Incident and Ongoing Investigation

[City, State] – [Date] – [Your Company Name], a [industry/type of business] company, is responding to a cybersecurity incident that was detected on [date]. Our team of experts is actively investigating the situation and taking steps to contain the incident.

While we continue to investigate the full scope of the incident, we want to assure our customers, partners, and the public that we are committed to resolving this matter as quickly as possible. At this time, we have taken steps to secure our systems, and we are working with cybersecurity professionals to prevent further disruption.

**What We Are Doing:**

* Our Incident Response Team has been mobilized to investigate and mitigate the impact.
* We are notifying affected individuals and providing them with resources to protect their personal information.

**What We Ask of the Public:**

* We advise individuals to remain vigilant and monitor their accounts for unusual activity.
* If you have concerns or questions, please contact our support team at [contact information].

We deeply regret any inconvenience caused by this incident and are committed to strengthening our security systems to prevent future occurrences. We will provide updates as the investigation progresses.

For more information, please contact: [Your Name]
[Your Title]
[Your Company Name]
[Phone Number]
[Email Address]
[Company Website]

These templates should help guide your communication during a cybersecurity incident. They ensure clarity, professionalism, and consistency while addressing the needs of different stakeholders. Make sure that the messages are customized for each specific situation and audience.

**Incident Response Form**

**General Information**

* **Incident Reported By:**
Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Title/Role: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Contact Information: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Incident Detection Date/Time:**
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Time: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Incident Identifier (Case Number):**
* **Incident Type:** (Select one or more)
	+ Malware/virus infection
	+ Phishing or spear phishing
	+ Unauthorized access or breach
	+ Denial of Service (DoS/DDoS) attack
	+ Data exfiltration
	+ Insider threat
	+ Other (specify): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Systems/Assets Affected:**

**Incident Details**

* **Incident Description:**
(Provide a detailed description of the incident, including how it was detected, affected systems, and any initial observations.)
* **Suspected Attack Vector:**
(How was the attack carried out? E.g., email, compromised website, USB drive, etc.)
* **Threat Actor Information (if available):**
	+ Name/Group: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	+ IP Addresses: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	+ Domains: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	+ Other Identifiers: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Severity Level (Select one):**
	+ Low
	+ Medium
	+ High
	+ Critical

**Containment Actions Taken**

* **Short-Term Containment:**
(List the immediate actions taken to isolate and contain the incident, e.g., disconnecting systems, blocking IPs, etc.)
* **Long-Term Containment:**
(List actions taken to prevent the incident from spreading, e.g., changing access credentials, restricting network access, etc.)

**Eradication Actions Taken**

* **Malware/Threat Removal:**
(Describe the actions taken to remove the threat, such as cleaning malware, eliminating unauthorized access, etc.)
* **System/Service Restoration:**
(List steps taken to restore affected systems, e.g., restoring from backups, reimaging systems, etc.)

**Recovery Actions Taken**

* **System/Service Recovery:**
(Describe the steps taken to reintegrate systems into production and ensure they are secure, including system checks and additional monitoring.)
* **User Notification:**
(If applicable, indicate if users were notified, and describe the content and scope of those notifications.)
* **Ongoing Monitoring:**
(Describe any additional monitoring or safeguards put in place to ensure no further incidents occur.)

**Communication & Reporting**

* **Internal Communication:**
(List the individuals and departments notified, and the method of communication used.)
* **External Communication:**
(Describe notifications sent to customers, partners, vendors, or regulatory bodies, if applicable.)
* **Regulatory Reporting (if applicable):**
(If the incident requires reporting to regulatory bodies, indicate which bodies were notified and when.)

**Impact Assessment**

* **Data Compromise:**
(List any data that was compromised or accessed, including personal data, financial information, etc.)
* **Business/Operational Impact:**
(Describe any downtime, disruption, or loss of revenue due to the incident.)
* **Legal/Compliance Impact:**
(Assess whether the incident impacts any legal or compliance requirements, such as GDPR, HIPAA, etc.)

**Root Cause Analysis**

* **Root Cause of Incident:**
(Explain the primary cause of the incident, e.g., vulnerability, human error, misconfiguration, etc.)
* **Lessons Learned:**
(What insights have been gained from this incident? Include any weaknesses identified in security practices, policies, or systems.)

**Post-Incident Actions**

* **Preventive Measures Implemented:**
(List any steps taken to prevent similar incidents, such as system hardening, employee training, etc.)
* **Security Enhancements:**
(Describe any new security controls or tools deployed to strengthen defenses.)
* **Employee Training & Awareness:**
(If relevant, describe any planned training or awareness campaigns for employees to mitigate future risks.)

**Incident Closure**

* **Incident Closed By:**
Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Date of Closure: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Final Status:**
	+ Resolved
	+ Under Control
	+ Open – Monitoring
	+ Escalated to Legal/External Experts
* **Incident Report Submitted:**
	+ Yes
	+ No
	+ Date Submitted: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Notes/Additional Comments:**

**Form Completion Confirmation**

* **Completed by:**
Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This **Incident Response Form** is designed to capture all relevant information during the lifecycle of an incident, ensuring all steps are well-documented for internal analysis, regulatory reporting, and future improvements. You can customize this form as needed based on your organization’s specific needs and incident response procedures.

