INCIDENT REPORTING TEMPLATE

Structured Approach to Incident Response and Recovery

Prepared by :
NIRANJAN V
ISO 27001 MENTOR

INCIDENT RESPONSE FORM

INCIDENT REPORT INFORMATION			
Full Name	<Full name of the person requesting the change>	**Contact Details**	<Email address, phone number, or any other relevant contact details>
Role/Designation	<Specify the requester's role or position>	**Department**	<Specify the requester's department>
Phone Number	<Specify the requestors Phone Number>	**Email ID**	<Specify the requestors Email ID>

© NIRANJAN V

INCIDENT DETAILS			
Incident Number/ Incident ID	<Assign a unique identifier for tracking purposes>	**Source of Incident**	<Specify the whether the incident is internal or external>
Date/Time of Incident Occurrence	<Specify the date and time when the incident actually occurred>	**Date/Time of Incident Detection**	<Specify the date and time when the incident was detected>
Incident Type	<Specify the type of incident, for example Malware Attack, Data Breach, Phishing Attempt, Physical Security Breach etc.>		
Incident Description	<Provide brief explanation of the incident specifying what happened>		
Incident Location	<Specify the location where the incident occurred, if applicable>		
Impact	<Describe the impact of the incident on the organization, including any systems affected, data compromised, or operations disrupted>		
Departments/Business Units Impacted	<Provide details of all the Departments/Business Units that are affected by the incident>		
Systems Impacted	<Provide details of all the systems that are affected by the incident>		
Processes Impacted	<Provide details of all the Processes that are affected by the incident>		

NIRANJAN V

Follow for more such Infosec Content & Reach out for ISO 27001 Mentorship, Training, and Guidance.

INCIDENT RESPONSE FORM

Customers Impacted	<Provide details of all the Customers that are affected by the incident>

INCIDENT SEVERITY

☐ **CRITICAL** ☐ **HIGH** ☐ **MEDIUM** ☐ **LOW**

© NIRANJAN V

INCIDENT NOTIFICATION

Incident Response Team Member first notified	**IT Head**	**Security Head**
<NAME>	<NAME>	<NAME>
<Position>	<Position>	<Position>
<Contact Information>	<Contact Information>	<Contact Information>
Application/Asset Owner	**Application/Asset Vendor**	**Human Resource**
<NAME>	<NAME>	<NAME>
<Position>	<Position>	<Position>
<Contact Information>	<Contact Information>	<Contact Information>
Legal Head	**Customers**	**Regulatory Bodies**
<NAME>	<NAME>	<NAME>
<Position>	<Position>	<Position>
<Contact Information>	<Contact Information>	<Contact Information>

NIRANJAN V

Follow for more such Infosec Content & Reach out for ISO 27001 Mentorship, Training, and Guidance.

INCIDENT RESPONSE FORM

INCIDENT RESPONSE DETAILS	
Quarantine Process	<Describe the actions taken to quarantine the assets and applications affected from the incident>
Immediate Actions	<Describe any immediate actions taken to contain the incident or mitigate its impact>
Root Cause Analysis	<Provide brief explanation of how the root cause analysis was performed>
Eradication	<Outline the steps planned or underway to remediate the incident and prevent future occurrences>
Impact	<Describe the impact of the incident on the organization, including any systems affected, data compromised, or operations disrupted>
Departments/Business Units Impacted	<Provide details of all the Departments/Business Units that are affected by the incident>
Systems Impacted	<Provide details of all the systems that are affected by the incident>
Processes Impacted	<Provide details of all the Processes that are affected by the incident>
Customers Impacted	<Provide details of all the Customers that are affected by the incident>

© NIRANJAN V

INCIDENT RECOVERY DETAILS	
Recovery Actions	<Describe the actions taken to restore affected systems, data, or services to their normal state>
Recovery Timeframe	<Specify the estimated or actual timeframe for completing the recovery process>
Post Recovery Verification	<Outline any verification steps taken to ensure that systems are fully restored and operational>
Communication	<Detail the communication plan for informing stakeholders, employees, and customers about the progress of the recovery process and any changes to business operations>

NIRANJAN V

Follow for more such Infosec Content & Reach out for ISO 27001 Mentorship, Training, and Guidance.

INCIDENT RESPONSE FORM

INCIDENT EVIDENCE COLLECTION	
Evidence Documentation	<Provide details on the types of evidence collected, their relevance to the incident, and their significance in the investigation>
Forensic Tools and Techniques	<Outline the forensic tools and techniques used to analyze digital evidence and identify the root cause of the incident>
Chain of Custody	<Document the chain of custody for collected evidence, including the individuals responsible for handling, and storing the evidence>

© NIRANJAN V

INCIDENT FORENSICS	
Forensic Investigation	<Specify if a formal forensic investigation is conducted and describe the scope and objectives of the investigation >
Evidence Preservation	<Describe the steps taken to preserve digital evidence related to the incident, including data logs, system snapshots, and network traffic captures>
Chain of Custody	<Document the chain of custody for collected evidence, including the individuals responsible for handling and storing the evidence>

LESSONS LEARNED	
Lessons Learned	<Document the lessons learned from the incident, including key takeaways and insights gained during the incident response process>
Recommendations for Improvement	<Provide recommendations for improving security controls, processes, or policies to prevent similar incidents in the future>
Action Plan	<Develop an action plan with specific tasks, responsible parties, and timelines for implementing the recommended improvements>

NIRANJAN V

Follow for more such Infosec Content & Reach out for ISO 27001 Mentorship, Training, and Guidance.

INCIDENT RESPONSE FORM

ATTACHMENTS (if applicable)
<List any supporting documents, logs, or evidence related to the incident>

© NIRANJAN V

INCIDENT REVIEW AND APPROVAL	
Reviewed By	**Approved By**
<NAME>	<NAME>
<Position>	<Position>
<Contact Information>	<Contact Information>

NIRANJAN V
Follow for more such Infosec Content & Reach out for ISO 27001 Mentorship, Training, and Guidance.

REACH OUT FOR ISO 27001 TRAINING MENTORING & GUIDENCE

NIRANJAN V

FOLLOW FOR MORE SUCH INFOSEC CHECKLIST, TEMPLATES AND DOCUMENTS