# Cyber Security Incident Response Template

Summary

The Cyber Security Incident Response Template provides the framework for managing security incidents reported by clients. It includes essential details about the incident, customer reporting specifics, an assessment of incident severity, actions taken, and a communication plan. This template ensures a systematic approach to documenting incidents, facilitating effective response and follow-up actions while also addressing compliance and regulatory requirements.

# End user steps:

Client Incident Reporting Guide

To ensure a prompt and effective response to cyber security incidents, clients should follow these steps when reporting an issue:

1. Identify the Incident

* Determine the nature of the issue and gather relevant details. Common ways issues are identified include:
  + Clicked a Suspicious Link: (If you clicked on a link in an email or message that appeared malicious.)
  + Entered Login Details on a Phishing Site: (If you provided your username and password on a site that you later recognised as fraudulent.)
  + Opened a Malicious Email Attachment: (If you downloaded and opened an attachment that you suspect contained malware.)
  + Observed Unusual System Behaviour: (If you noticed strange pop-ups, system slowdowns, or unauthorized changes to your files or settings.)

Gather Key Details:

* Date and Time of Incident: (When the issue was first observed.)
* Person or people affected
* Affected Systems: (Which systems, applications, or accounts are impacted.)
* Description of the Incident: (Provide a brief overview of what occurred (e.g., "I clicked a link in a phishing email and entered my login credentials").

2. Report the Incident

* Contact the Service Desk: (Reach out using the designated method (e.g., phone, email, or ticketing system).
* Provide Your Information: (Include your name, email address, and phone number for follow-up.)
* Indicate Reporting Method: (Specify how you are reporting the incident (e.g., via email or through the ticketing system).
* Time Frame: (Note the time between when the incident was first observed and when it was reported.)

3. Incident Severity Assessment

* Assess Severity: Assist in determining the severity of the incident, which may be categorised as low, medium, high, or critical based on its potential impacts (e.g., data loss, unauthorized access, operational disruption).
* Document Actions Taken
* Keep Records: Note any immediate actions you’ve taken, such as:
  + Changing passwords for affected accounts.
  + Enabling multi-factor authentication (MFA) where possible.
  + Running antivirus or anti-malware scans.
  + Reporting any suspicious communications to your IT or security team.

# Security Team Steps:

Incident Details

* Date and Time of Incident Reported:
* Nature of Incident:
* Affected Systems:
* Description of Incident:

Customer Reporting Details

* Customer Name:
* Contact Information:
* Method of Reporting: (e.g., email, phone call, ticketing system)
* Time Frame of Reporting: (e.g., when the incident was first observed vs. when it was reported)

Incident Severity Assessment

* Severity Level: (e.g., low, medium, high, critical)
* Impact Assessment: (e.g., data loss, operational disruption, financial loss, reputational impact)

# Incident Response Team

* Team Members Involved: (Names and roles)
* Contact Information: (Emails and phone numbers)

Timeline of Events

* Detailed Timeline:
  + Incident Discovery:
  + Incident Reporting:
  + Investigation Start Time:
  + Actions Taken:
  + Incident Resolution:
* Duration of Incident: (Total time from detection to resolution)

## Investigation Steps

Steps Taken to Identify the Issue:

1. Audit Log Review:
2. Account Permissions and Access Review:
3. Roles and Privileges Assessment:
4. Authentication Methods Review:
5. Network Traffic Analysis: (If applicable)
6. Malware Scanning: (If applicable)

Actions Taken

* Password Changes:
* MFA Revocation:
* Reauthentication Request:
* Password Reset Notifications:
* Authentication Method Update:
* Self-Service Password Reset Configuration:
* MFA Configuration:
* User Communication: (Informing affected users)
* Incident Containment Measures: (Steps taken to contain the breach)

## Communication Plan

* Internal Communication:
  + Who was informed and when?
  + Communication methods used (e.g., meetings, emails).
* External Communication:
  + Customer notifications or press releases.
  + Regulatory notifications, if applicable.

## Follow-Up Actions

The following actions should be considered as part of a formal response to a major incident.

* Write a major incident report and circulate it to senior management
* Post-Incident Review: (Plan for a review meeting)
* Additional Training Needs: (Identify gaps in knowledge)
* Improvement Measures: (Steps to prevent recurrence)

Regulatory and Compliance Considerations

* Compliance Requirements: (Relevant laws and regulations)
* Reporting Obligations: (Mandatory notifications to authorities, if applicable)

Tools and Resources Used

* Incident Response Tools: (List of software and tools utilised)
* Documentation Resources: (Reference materials or guidelines)

Lessons Learned

* Key Takeaways: (Insights gained from the incident)
* Improvements to Security Posture: (Changes to be made based on findings)

## Conclusion

Next Steps

* Service Proposal: (Outline proposed actions for the future)
* Follow-Up Meetings: (Schedule for future reviews or follow-ups)

Final Approval

* Reviewed By: (Names and signatures of reviewing personnel)
* Date of Approval: