Cyber Security Incident Assessment Form Sample

The **cyber security incident assessment form sample** is designed to help organizations systematically evaluate and document security breaches. It enables efficient identification of threats, impact analysis, and corrective action planning. This form is essential for maintaining robust incident response protocols.

1. Incident Identification

Incident ID	e.g., INC-2024-001
Date/Time Detected	
Detected By	Name or Department
Point of Contact	Contact Person

2. Incident Description

Brief description of the incident

3. Threat Identification

Type of Incident	Select
Systems Affected	e.g., Server names, devices
Detection Method	e.g., SIEM, antivirus, user report

4. Impact Analysis

Data Compromised	☐ Confidentiality ☐ Integrity ☐ Availability
Scope/Severity	Select
Potential Impact	Describe possible consequences

5. Response Actions

Immediate Actions Taken	e.g., isolated systems, changed passwords
Additional Recommendations	e.g., user training, system updates
Escalation	Select

6. Final Assessment & Follow-up

Resolved?	Select
Follow-up Actions	e.g., audit, review security policies

Prepared by:

Your name

Date:

This form is for internal use only and should be handled according to your organization's data protection policies.