Network Security Incident Identification Template

Incident Overview

Incident ID / Reference	
Date & Time Identified	
Incident Reporter (Name/Contact)	
Department / Location	

Incident Description

Summary of Incident	
Date & Time of Event (if known)	
Detection Method	
Systems/Devices Impacted	
Network Segments Involved	

Indicators & Evidence

Observed Indicators	
Supporting Logs/Evidence	

Initial Impact Assessment

Potential Data Exposed	
Estimated Severity	
Affected Users/Departments	

Next Steps & Recommendations

Immediate Actions Taken	
Suggested Actions	
Reported To (Teams/Authorities)	

Prepared by

Name	
Date	
Signature	