To: [Recipient Name/Regulatory Body]

From: [Your Name/Organization Name]

Date: [Date of Report]

Subject: Detailed Description of Security Incident - [Incident Reference Number]

1. Incident Overview

Type of Incident: [e.g., Data Breach, Malware, Unauthorized Access]
Date/Time of Discovery: [Date and Time]
Estimated Date/Time of Occurrence: [Date and Time]

2. Description of the Incident

[Provide a chronological narrative of how the incident occurred. Describe the point of entry, the methods used by the unauthorized party, and the timeline of suspicious activity observed.]

3. Systems and Data Affected

Affected Systems: [List specific servers, applications, or hardware involved]
Types of Data Involved: [e.g., Personal Identifiable Information (PII), Financial Records, Intellectual Property]
Number of Records Impacted: [Estimated number of affected individuals or files]

4. Root Cause Analysis

[Explain the underlying vulnerability or cause that allowed the incident to happen, such as a software bug, human error, or compromised credentials.]

5. Containment and Mitigation Actions

[Describe the immediate steps taken to stop the incident and limit damage. Include technical measures like isolating systems, resetting passwords, or patching vulnerabilities.]

6. Impact Assessment

[Detail the consequences of the incident on business operations, data integrity, and privacy of the affected parties.]

7. Remediation and Future Prevention

[Outline the long-term strategy to prevent a recurrence, including policy changes, additional security training, or new technical safeguards.]

8. Contact Information

For further inquiries regarding this incident, please contact:
Name: [Contact Name]
Role: [Contact Title]
Email: [Email Address]
Phone: [Phone Number]

Sincerely,

[Signature]
[Printed Name]
[Title]