**Cybersecurity Templates**

**Intern Incident Report**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Intern Incident Report** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document ID:** | [INC‑YYYY‑####] | **Report Type:** | [Initial / Update / Final] |
| **Date/Time of Report (UTC):** | [YYYY‑MM‑DD HH: MM] | **Confidentiality:** | [Internal / Confidential / Restricted] |

Contents

[Intern Cybersecurity Incident Report 3](#_Toc207322885)

[Section A — Parties & Context (Reporter) 3](#_Toc207322886)

[Section B — Incident Snapshot 3](#_Toc207322887)

[Section C — Factual Description (≤150 words) 3](#_Toc207322888)

[Section D — Impact (Initial) 3](#_Toc207322889)

[Section E — Immediate Actions (Reporter / Supervisor) 4](#_Toc207322890)

[Section F — Technical Investigation (Incident Lead) 4](#_Toc207322891)

[Section G — Evidence & Chain of Custody (Incident Lead) 4](#_Toc207322892)

[Section H — Communications & Notifications 5](#_Toc207322893)

[Section I — Root Cause, Lessons, and Actions (Close‑out) 5](#_Toc207322894)

[Section J — Approvals 5](#_Toc207322895)

[Guidance for Intern‑specific Context 5](#_Toc207322896)

# Intern Cybersecurity Incident Report

Use this form to record cybersecurity-related incidents involving interns (as reporters, witnesses, or subjects). Keep entries factual and time-stamped. Bracketed items are placeholders. Sections A–E are completed by the reporter/manager; F–H by the Incident Lead.

# Section A — Parties & Context (Reporter)

* **Reporter Name & Role:** [Intern / Supervisor / Peer / Other]
* **Reporter Contact:** [email/phone]
* **Intern(s) Involved:** [Name, program, start–end dates]
* **Supervisor / Mentor:** [Name, dept]
* **Business Unit / Project:** [Team, system or app]
* **Location/Environment:** [On-site / Remote / Hybrid; Region/Time zone]
* **Relationship to Organisation:** [Employee / Intern / Contractor / Volunteer / Partner]

# Section B — Incident Snapshot

* **Date/Time First Observed (UTC):** [YYYY‑MM‑DD HH:MM]
* **Date/Time Reported:** [YYYY‑MM‑DD HH:MM]
* **Detection Source:** [User report / SOC / EDR / SIEM / Third‑party]
* **Incident Type (select all):** [Phishing / Malware / Ransomware / BEC / Account compromise / Data exposure / Web app / DoS/DDoS / Insider / Misconfiguration / Third‑party / Other]
* **Status (initial):** [Pending / Confirmed / Contained / Recovering]
* **Severity (initial):** [Low / Medium / High / Critical]

# Section C — Factual Description (≤150 words)

* **What happened?** [Concise facts only]
* **Where did it occur?** [System/asset, repo, tenant, URL]
* **How was it noticed?** [Alert/ticket, who observed]
* **Who is affected?** [Users/accounts, customers, partners]
* **Known Indicators (IoCs/TTPs):** [Domains, IPs, hashes, MITRE tags]

# Section D — Impact (Initial)

* **Confidentiality:** [None / Limited / Sensitive / Regulated]
* **Integrity:** [None / Minor / Moderate / Major]
* **Availability:** [None / Degradation / Outage]
* **Business Impact (early view):** [Minimal / Moderate / Significant / Severe]
* **Personal Data Involved?** [Yes/No/Unknown] If Yes → **Type:** [PII / PCI / PHI / Other]

# Section E — Immediate Actions (Reporter / Supervisor)

* **Containment Taken:** [Isolated host, blocked domain, password reset, token revoke]
* **Medical/Wellbeing or Safeguarding Needs:** [If the incident includes harassment/bullying, escalate per safeguarding process]
* **People Notified:** [Manager, SOC, HR, Legal, Privacy, Comms]
* **Attachments/Evidence:** [Screenshots, log extracts, ticket IDs]

# Section F — Technical Investigation (Incident Lead)

* **Initial Vector:** [Email / Web / Credentials / Supply chain / Insider / Other]
* **Accounts/Identities Affected:** [Users, service accounts]
* **Assets/Systems Affected:** [Hostnames/IDs, cloud account, repository]
* **Lateral Movement/Persistence:** [Observed techniques]
* **Data at Risk or Exfiltration Evidence:** [Yes/No + details]
* **Timeline of Events (UTC):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Timestamp** | **Source** | **Event/Action** | **Owner** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

# Section G — Evidence & Chain of Custody (Incident Lead)

* **Register:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item ID** | **Description** | **Source/Tool** | **Collected By** | **Collected At (UTC)** | **Hash (Algo)** |
|  |  |  |  |  |  |

* **Preservation & Access Controls:** [Storage location, who has access]
* **Transfers:** [When, to whom, purpose]

# Section H — Communications & Notifications

* **Internal Updates:** [Times, audiences, channels]
* **External Notifications (if applicable):** [Regulator / Customer / Law enforcement]
* **Safeguarding/Conduct Pathway:** [If interpersonal/transgressive behaviour is alleged, log in HR/safeguarding system and record case ref]

# Section I — Root Cause, Lessons, and Actions (Close‑out)

* **Root Cause:** [Human error / Control failure / Vulnerability exploit / Third‑party / Unknown]
* **Contributing Factors:** [Bullets]
* **Lessons Learned:** [Bullets]
* **Corrective & Preventive Actions:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Owner** | **Due** | **Evidence** |
|  |  |  |  |

* **Residual Risk:** [None / Low / Medium / High]
* **PIR Scheduled Date:** [YYYY‑MM‑DD]

# Section J — Approvals

* **Incident Lead:** [Name, date]
* **System Owner:** [Name, date]
* **Security Leader:** [Name, date]
* **HR/People Partner (if safeguarding case):** [Name, date]

# Guidance for Intern‑specific Context

* **Scope of duties:** note whether the intern acted within assigned duties or unsupervised work.
* **Access level:** record assigned privileges (least privilege expected) and any emergency elevations.
* **Training status:** confirm completion of security awareness and relevant tooling onboarding.
* **Supervision:** identify supervising staff present or on‑call at the time.

**Drop-down Vocabularies (suggested)**

* **Detection Source:** User, SOC, SIEM, EDR, MSSP, Third‑party, Law enforcement
* **Status:** Pending, Confirmed, Contained, Recovering, Resolved, Closed
* **Data Sensitivity:** Public, Internal, Confidential, Restricted

**Footnotes**

* Keep content factual; avoid speculation. For safeguarding/behavioural allegations, use your organisation’s dedicated speak‑up channel, maintain confidentiality, and record only the minimum necessary personal data in this report.