**Description of suspected/potential incident**

**Who discovered the incident:** Click or tap here to enter text.

**Who or What (is this affecting)** Click or tap here to enter text.

**When (did this occur)** Click or tap here to enter text.

**What (happened)** Click or tap here to enter text.

**Cause(s) of the issue**

**Main cause(s):** *Examples include Credential & Identity Compromise, Configuration & Human Error, Exploitation & Vulnerabilities, Device & Asset Loss, Advanced & Targeted Attacks, Fraud & Deception, Insider Threats):* Click or tap here to enter text.

**Root Cause** *(Initial compromise not when you were first alerted, if it’s the same then fill in the same information.:* Click or tap here to enter text.

* **Patient Zero** Click or tap here to enter text.

**Risk or Exposure of potential incident**

**Provide details on data that may have been accessed or taken.** Click or tap here to enter text.

**Value of the Asset/All users or applications effected** Click or tap here to enter text.

**Potential Scope and Impact:** *What would the loss or felt impact be if the incident were real and fully realized? How many people would this effect?* Click or tap here to enter text.

**Likelihood of Impact: What is the risk?(Indicate High/Medium/Low):** *Example of high might be access to the full client database vs. low might be a proprietary internal process document with limited intellectual property.* Click or tap here to enter text.

**Has data been exposed or not? How certain are we?**Click or tap here to enter text.

**Collection of evidence**

**Please provide evidence that substantiates or supports the cause and risk or exposure of the incident?** *(Eyewitness, time-stamped logs, screenshots, video footage, etc)*Click or tap here to enter text.

**What log/data sources were collected?** *Examples could include**M365 UAL, EDR/MDR/XDR logs, SIEM exports, cloud logs, third party logs, etc.* Click or tap here to enter text.

**Who currently holds the evidence? Provide name and contact information.** Click or tap here to enter text.

**How is the evidence being/has been protected?** Click or tap here to enter text.

**Describe recommended containment and remediation activities**

**Containment Actions:** *What actions did you take to stop the bleeding. Isolate device(s), turn off internet, remove server from external access, disable account, remote wipe a device(s), etc. Please indicate what actions you took to contain:* Click or tap here to enter text.

**Recommended steps to reduce impact:** *Notify management and legal teams (IHT), communicate issue to employees or customers as needed.* Click or tap here to enter text.

**Recommended remediation (fix):** Implement a patch or configuration change, reset user credentials, deploy multi-factor, etc. Click or tap here to enter text.

**Communicate to Leadership – Executive Summary**

**Communicate to all parties with knowledge of the incident to treat information about the incident as sensitive or confidential. Please list who has knowledge of the incident.**

Click or tap here to enter text.

**Explain what happened and why this is important to our business.** Click or tap here to enter text.

**What is the risk if we fail to act?** Click or tap here to enter text.

**Immediate Actions Taken:** *Specific responses or actions and why. The responses or action(s) taken, provide reduced impact or liability?* Click or tap here to enter text.

**Proposed Remediations: Are there follow-up risks that require additional action(s**)**?** *Example, communication strategy, user awareness activities, process changes, systems/tools enhancements or implementations (long-term actions). Present to leadership for approval of action(s) or response(s)* Click or tap here to enter text.

**Identify next steps**

**Establish the category and severity of the incident:** *Do we have enough information to establish the category and severity of the incident? If yes, declare the category and severity. If no, describe what else might be required.*  Click or tap here to enter text.

**Confirmation of Notification:** *Confirm all parties have been notified, ensure all reporting deadlines are met (self-imposed or regulatory).* Click or tap here to enter text.

**Follow Up Actions?** Write out all actions still to be performed or reviewed and who is responsible. Click or tap here to enter text.

**Summary Report date and time:** Click or tap here to enter text.

**Form prepared by, with contact info:** Click or tap here to enter text.