**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry.  **05th June 2024** | **Entry:**  Record the journal entry number.  **1** |
| Description | Provide a brief description about the journal entry.  **Documenting a security incident (health care clinic)** |
| Tool(s) used | List any cybersecurity tools that were used.  Nil |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   An organized group of unethical hackers   * **What** happened?   The clinic computers were installed with ransomware, encrypting the organization’s critical files.   * **When** did the incident occur?   Tuesday morning at 9am   * **Where** did the incident happen?   Health care clinic   * **Why** did the incident happen?   The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. Attackers demand the company to pay a large sum of money in exchange for a decryption key. |
| Additional notes | Include any additional thoughts, questions, or findings.  What should the company do to prevent this incident from occurring again in the future? |

### Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

|  |
| --- |
| Reflections/Notes: Record additional notes. |