Incident management - Policy checklist

The following checklist aims to help entities thoroughly plan and manage incidents. It provides tasks and activities which need to be completed in each of the information security event and incident management phases.

#### Plan and Prepare

|  |  |
| --- | --- |
| 1. **Policy Section** | 1. **Checklist** |
| 1. Policy and planning  * Incident management policy published with senior management commitment. * Incident management policy is integrated and aligns with relevant policies such as BCP, DRP, and other risk management policy. * Identify and define the roles and responsibilities in incident management (incident response team, incident management team, executive leadership, etc). * Incident management team members selected and appointed. * Employee conduct defined, relevant internal controls and governance established. * Register of all systems and information assets and resources that are critical to operations created. * Communication plans for incident management developed. |  |
| 1. Incident management team and incident response team  * Incident management team and incident response team members are notified of appointment. * List of officers authorised to communicate with QGCSU; initiate request for CDC external assistance; complete and submit the incident reporting to QGCSU. * Training requirements for incident management team and/or incident response team outlined. |  |
| 1. Processes and procedures  * Establish security monitoring and alerting systems. * Procedures established to record, analyse, and escalate incidents. * Incident response playbooks developed and adopted. * Additional response procedures (including staff reporting procedures, incident management team phone/email response protocols) developed. * Prepare all procedure forms and tools that will be used during an incident response process including crisis communication plans and templates. * Outline communication strategies to engage with internal and external stakeholders directly related to incident management. |  |
| 1. Training  * Outline incident management team training regime for users, incident management team and incident response team members, and executive leadership. * Conduct employee training/informing employees on incident reporting. * Run consistent training programs to assist users. |  |
| Communications plan   * Create and maintain contact lists for incident management team and incident response plan members. * Establish and rehearse out of hours communications. * Determine the process to conduct internal briefings to executive and ministerial leadership. * Draft templates to be used for internal and external communications. * Outline the process to draft, approve, and release external communications. * Develop list of approved entity spokespersons. |  |
| 1. Testing and exercising  * Test incident management team response efficiency. * Test incident response processes and procedures. * Run employees through help desk scenarios. |  |

#### Detection and reporting

|  |  |
| --- | --- |
| 1. **Activity** | 1. **Checklist** |
| Detection   * Help desk support has been established. * After hours procedures have been established. * Automated monitoring and detection systems are in place. * Have defined processes depending on the detection source. |  |
| Logging and information capture   * The incident management team has been established and maintains a secure incident register and log. * The incident management team understands the importance of logging all activities during the incident response process. * All electronic evidence and information assets related to the event. |  |
| Initial reporting   * Define reporting procedures and contact points to the incident management team. * The responding team contacts the relevant parties within the department and other members as deemed appropriate in processes and playbooks. * The responding team and incident management team understands the defined escalation routes and triggers. |  |

#### Assessment and decision

|  |  |
| --- | --- |
| 1. **Activity** | 1. **Checklist** |
| Assessment   * Responding team follows the Incident reporting standard to assess the incident. * Follow defined escalation criteria based on the incident assessment. * Determine any reporting requirements based on the BILs of the system or information asset. * Define the incident and its impacts in clear and simple language. * Determine incident type, scope, and business impact. |  |
| Logging and information capture   * The incident response team and incident management team continue all logging activities during the incident response process. * The incident response team and incident management team capture all electronic evidence and information assets related to the event. |  |

#### Response

|  |  |
| --- | --- |
| 1. **Activity** | 1. **Checklist** |
| 1. Incident review  * Conduct ongoing assessment of the incident. * Arrange response activities as outlined in relevant playbooks. * The incident management team and incident response team should be aware of when to escalate or end the incident response activities (documented thresholds). |  |
| Forensic analysis   * The entity has monitoring/detection techniques for automated incident detection, which can be used for forensic analysis. * The entity can collect forensic data. * The entity has access to resources that would allow forensic analysis. |  |
| Logging and information capture   * The response team and incident management team continue all logging activities during the incident response process. * The response team and incident management team capture all electronic evidence and information assets related to the event. |  |
| Communications   * Communicate the status of the incident with relevant stakeholders. * Develop key messages for distribution to key audiences. |  |

#### Lessons learnt

|  |  |
| --- | --- |
| 1. **Activity** | 1. **Checklist** |
| 1. Post incident report  * Collect observations throughout an incident. * Conduct analysis on the observations and incident log/s. * Identify insights and arising lessons identified. * Produce the post incident review and distribute to the internal entity security governance body. * The incident response team and incident management team should complete the post incident review as soon as viable after the resolution of the incident. |  |
| 1. Processes and procedures review  * Policies, planning, and incident detection, response and reporting processes refined. * Tasks refined. * Responsibilities redefined. |  |