# Event and incident management policy checklist

The following checklist aims to help agencies thoroughly plan and manage information security 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  * information security incident management policy published with senior management commitment * ISIRT members selected and appointed * employee conduct defined * internal controls and governance established * any existing business continuity and ICT disaster recovery plans have been integrated with the incident management policy. |  |
| 1. ISIRT  * ISIRT team members are notified of appointment * external ISIRT members appointed and notified of their roles * the ISIRT is assembled * list of department officers authorised to communicate with QGISVRT; initiate request for VRT external assistance; complete and submit the incident reporting spreadsheet, supplied to QGCIO and QGISVRT. |  |
| 1. Processes and procedures  * incident response playbooks developed and adopted * additional response procedures (including staff reporting procedures, ISIRT phone/email response protocols) developed. * Prepare all procedure forms and tools that will be used during an incident response process |  |
| 1. Training  * ISIRT training * employee training/informing employees on incident reporting. * run consistent training programs to assist users |  |
| 1. Testing  * test ISIRT response efficiency * test incident response processes and procedures * run employees through help desk scenarios. |  |

#### Detection and reporting

|  |  |
| --- | --- |
| 1. **Activity** | 1. **Checklist** |
| Detection   * ISIRT 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 ISIRT has defined a secure incident register * the ISIRT understands the importance of logging all activities during the incident response process * the ISIRT captures all electronic evidence and information assets related to the event |  |
| Initial reporting   * define reporting procedures and contact points to the ISIRT * the ISIRT contacts the relevant parties within the department and other ISIRT members * the ISIRT understands the defined escalation routes and triggers |  |

#### Assessment and decision

|  |  |
| --- | --- |
| 1. **Activity** | 1. **Checklist** |
| Assessment   * ISIRT 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 BIL of the system or information asset * Incident assessments are defined in clear and simple language |  |
| Logging and information capture   * the ISIRT continues all logging activities during the incident response process * the ISIRT captures all electronic evidence and information assets related to the event |  |

#### Responses

|  |  |
| --- | --- |
| 1. **Activity** | 1. **Checklist** |
| 1. Incident review  * conduct ongoing assessment of the incident * arrange response activities and relevant playbooks * ISIRT should be aware of when to escalate or end the incident response activities |  |
| 1. Response activities  * the ISIRT exercises the defined processes from the relevant playbooks * conduct response activities to resolve the incident. |  |
| Forensic analysis   * the department has monitoring/detection techniques for automated incident detection, which can be used for forensic analysis * the department can collect forensic data * the department has access to resources that would allow forensic analysis |  |
| Logging and information capture   * the ISIRT continues all logging activities during the incident response process * the ISIRT captures all electronic evidence and information assets related to the event |  |

#### Lessons learnt

|  |  |
| --- | --- |
| 1. **Activity** | 1. **Checklist** |
| 1. Post incident report  * conduct analysis on the incident register and incident log * identify lessons learned * produce the PIR and distribute to the internal agency security governance body. * the ISIRT should complete the PIR as soon as viable after the resolution of the incident |  |
| 1. Processes and procedures review  * incident response process model refined * tasks refined * responsibilities redefined * incident detection and reporting procedures * ISIRT help desk policies improved. |  |