**Information Security Incident and Privacy Breach Response Plan**

### Overview

**1. Preparation**
Knowing how to respond to a security incident before it occurs can save valuable time and effort. Preparation includes team training, scenario exercises (paper and technical based), development and testing of new tools.

**2. Identification**
Identification involves identifying whether or not a security incident has occurred. If an incident has occurred, create an incident record in Eramba and apply an initial classification to the incident.

**3. Containment**
Containment involves limiting the scope and magnitude of a security incident.

**4. Eradication**
Eradication involves removing the cause of the security incident. It can involve, for example, malware removal, patching of vulnerabilities, or dismissal of staff.

**5. Recovery**
Recovery involves restoring services to normal operating status. Restoration of services and systems should be tested and verified.

**6. Lessons Learned**
Addressing some security incidents requires considerable time and effort. Performing a ‘lessons learned’ activity is important for all incidents.

---

**Definitions**

- **Security event**: An observable occurrence associated with a system, service or network state that occurs at a point in time and may be relevant to information security.

- **Security incident**: A single or series of unauthorised or unexpected security events resulting in, or indicating harm to, the organisation.

---

**Key Roles and Responsibilities**

**First responder**
First responders perform initial assessments of security events that have been reported or received via an alert. Typically first responders will be from the End User, IT Operations and Information Security teams.

**Incident classifier**
Incident managers oversee and prioritise responses in response to an incident. They ensure the incident is correctly classified and that escalations occur appropriately.

**Incident coordinator**
Incident coordinators are responsible for communicating with stakeholders and ensuring that incidents are managed effectively.

---

**Incident Classification**

<table>
<thead>
<tr>
<th>Categories</th>
<th>Types</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorised access</td>
<td>Targeted or Opportunistic</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Malware</td>
<td>Commodity or Advanced</td>
<td>Major</td>
</tr>
<tr>
<td>Improper action</td>
<td>External or Insider</td>
<td>Moderate</td>
</tr>
<tr>
<td>Denial of service</td>
<td></td>
<td>Low</td>
</tr>
</tbody>
</table>

---

**Incident Levels**

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

---

**Contacts**

- **Manager, Information Security**: Andrew Wheeler
- **IT End User Team Manager**: Peter Turnbull
- **Privacy Officer**: Melissa Lumley
- **Chief Information Office (CIO)**: Martin Richards
- **GM, Risk and Compliance**: Greg King
- **IT End User Team**
- **Security Team**
- **Corporate Risk Consequence Matrix**

---

**Use the Global Address List for phone numbers**

**Add to the Corporate Risk Consequence Matrix** for guidance on risk assessments and risk appetite settings.