[Insert organisation name/logo]

**CYBER SECURITY INCIDENT RESPONSE PLAN**

(*Source: Australian Signals Directorate* [*Australian Cyber Security Centre*](cyber.gov.au))

|  |  |
| --- | --- |
| 1. **Preparation checklist** | |
| * Have we identified the systems and data critical to our business operations? |  |
| * Do we have business continuity and disaster recovery plans? |  |
| * Do we have an up‐to‐date and regularly tested cybersecurity incident response plan? |  |
| * Do our agreements with service providers include cybersecurity incident reporting and response activities? |  |
| * Do we have the ability to detect when cybersecurity incidents may have occurred? |  |
| * How easily and quickly can we access appropriate resources to respond to cybersecurity incidents? |  |
| * What are our legislative obligations in regard to reporting cybersecurity incidents? |  |
| * Do we have a public communications plan in case of cybersecurity incidents? |  |

|  |
| --- |
| 1. **Reporting cybersecurity incidents** Depending on the level and severity of the incident, **[insert organisation name]** will[report the incident to ASD](https://www.cyber.gov.au/report-and-recover/report/report-a-cyber-security-incident#no-back). The types of cybersecurity incidents that should be reported to ASD include: |
| * suspicious privileged account lockouts * suspicious remote access authentication events * service accounts suspiciously communicating with internet-based infrastructure * compromise of sensitive or classified data (data breach) * unauthorised access or attempts to access a system * emails with suspicious attachments or links * denial-of-service attacks * ransomware attacks * suspected tampering of electronic devices.   *NOTE: Under the limited use obligation, information voluntarily provided to ASD about cybersecurity incidents, potential cybersecurity incidents or vulnerabilities impacting organisations cannot be used for regulatory purposes.* |

|  |  |
| --- | --- |
| 1. **Communication checklist**   **[insert organisation name]** will communicate publicly about cybersecurity incidents after taking into account the below. | |
| * Person responsible for *producing* information about the cybersecurity incident |  |
| * Person responsible for *approving* the release of information about the cybersecurity incident |  |
| * Person responsible for *communicating* information about the cybersecurity incident |  |
| * Have clear and consistent communications channels to communicate information about the cybersecurity incident |  |
| * Opportunities for media, clients, stakeholders, and the broader public to make enquiries regarding the cybersecurity incident (e.g. via email, telephone hotlines or social media) |  |