Managed Service Provider Better Practice Principles

December 2018 (Version 1.0)

This document specifies the Australian Cyber Security Centre (ACSC) better practice principles for Managed Service Providers (MSPs). MSPs commit to these principles as a requirement of joining the ACSC Managed Service Provider Partner Program (MSP[3]).

As a managed service provider:

We prioritise cyber security in everything we do

- Implement security measures during all stages of ICT system and network development, deployment, and maintenance.
- After implementing recommended risk mitigations, review and accept residual cyber security risks before authorising systems and networks to operate in production environments.
- All changes to ICT systems and networks are recorded, reviewed, and approved before implementation.
- Cyber security is a core requirement for procuring software, hardware, and services, including cloud services.

We implement better practice cyber security guidance and standards

- Implement the ACSC's Essential Eight mitigation strategies at maturity level three.
- Implement the ACSC's Secure Administration, and Network Segmentation and Segregation guidance.
- Implement an industry recognised cyber security governance framework.

We protect the confidentiality, integrity, and availability of our data, and our customers' data

- Perform daily backups of important data.
- Store backups for at least 3 months.
- Store backup media offline or disconnected from the network, or online but in a non-rewritable and non-erasable manner.
- Conduct partial recovery tests of backups annually or more frequently.
- Implement and test a business continuity plan, and disaster recovery plan.

We educate our staff about cyber security

- Provide contemporary cyber security awareness training to new staff.
- Provide contemporary cyber security awareness training to all staff annually or more frequently.
- Provide tailored cyber security awareness training for staff more likely be targeted in a cyber-attack. Broadly this can include senior managers, system administrators, and finance and HR personnel.

We act ethically and responsibly with our customers' data and cyber security

- Segregate customer networks logically and physically from each other and from the MSP network.
- Implement multi-factor authentication for all access to customer systems.
- Have upfront and transparent cyber security conversations with customers.
- Apply security patches and mitigate vulnerabilities within ACSC's recommended timeframes.
- Report all confirmed cyber security incidents and data breaches to impacted customers and the ACSC within 48 hours.
- Report all data breaches that are likely to result in serious harm to individuals as soon as practicable to the Office of the Australian Information Commissioner.

We practice secure administration with our systems, and our customer's systems

- Restrict administrative privileges using role based access.
- Use multi-factor authentication for privileged users.
- Use hardened jump boxes and dedicated privileged user workstations exclusively for privileged tasks.
- Use complex and unique passphrases and store passphrases in a secure and centralised password management tool.
- Log all use of privileged accounts, including access and modifications to data and systems. Review the logs for unusual activity.

We are prepared for cyber security incidents

- Create an Incident Response Plan and exercise it annually or more frequently.
- Log security events to a secure centralised logging solution such as a Security Information and Event Management solution.
- Retain event logs for a minimum of 7 years.
- Review event logs daily for unusual activity.
- Train all staff on how to respond to a cyber security incident.

We regularly review and improve our cyber security

- Regularly assess the cyber security of ICT systems and networks.
- Continually monitor cyber security risks and posture.
- Complete the Managed Service Provider Better Practice Survey and provide it to the ACSC.