

Data Security Policy

Our commitment

AMH Civil and its leadership is committed to building and managing a company with systems and infrastructure in place to ensure the security and integrity of internal data, to ensure we remain a trusted partner for our clients and stakeholders to share data with, and to comply with industry and government regulations and guidelines with regard to data security.

Data Security Policy in practice

In the development of systems and the implementation of hardware and software we will consider the following in order to best mitigate data security issues and potential breaches:

- Review and consideration of appropriate levels of control in accordance with the Australian Cyber Security Centre Essential Eight framework
- Remote monitoring and management in place as appropriate for business IT hardware
- Multi factor authentication in place for all AMH Civil user profiles
- Use of trusted software with demonstrated commitment to data security
- Register of approved software maintained by the business
- Appointment of General Manager as the internal Data Security Officer
- Appropriate use of on site hardware with built in router firewall
- Blocked sign in for shared mailboxes to ensure traceable and secure log in activity
- Records maintained of suspicious activity and security breaches on incident register
- Security breaches reported to affected parties and to Ombudsman as required under law
- Threat detection and management software implemented within Business IT Systems
- Data sharing approvals and access managed through Document Control Procedure and position descriptions

Policy Reviews

We may from time to time review and revise our policies. Accordingly, we reserve the right to change this Policy at any time.

A handwritten signature in black ink, appearing to read 'JM' or similar initials, followed by a flourish.

Joseph Mansell

General Manager / Director

AMH Civil