SECURITY POLICY – CLOUD HOSTING

Approving Authority	Mark Cassidy, Managing Director
Version	V2.0. March 2020
Next scheduled review	January 2021
Document Number:	SP2CR0098
Description	This document sets out the principals, objectives and responsibilities for externally hosting services or data by anyone within the organisation.

- MWH – My Workplace Health
- HRMS – Health Risk Management System Pty Ltd (owner of the software)
- 2CRisk – previous name of software
- 2CRisk Holdings – Holding Company where IP is vested.

1. DEFINITIONS

a) Internally hosted and MWH (My Workplace Health) cloud services are data and information storage hosting services that are maintained and cloud based. These include:

a. MWH Google Drive (2FA)
b. Panther Email exchange platform (2FA)
c. Zero payroll and accounting platform (2FA mandatory)
d. cPanel Website
e. Adobe Cloud suite

b) External hosting, commonly known as cloud computing, is where some or all components of the service are provided and managed by third parties. Externally hosted for MWH relates to the delivery of our software solution to the marketplace and include:

a. Bit Bucket code repository
b. Oracle 12G database
   i. Development Environment
   ii. Test Environment
   iii. Production Environment
c. Amazon Web Services (AW) hosting
d. APEX Environment (Application Express)
e. Imperva Cloud Security platform

Further information on AWS cloud hosting security can be found at:

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html

For access to all of the above components:

- All solutions can only be accessed by VPN
- Internally owned VPN's are mandatory
- Only the CTO can issue VPN access with approval from MD
- Multi Factor Authentication must be utilised
- MFA via 2 sources. Password via email and authentication via text
- Passwords changing – mandated for 30 days cycle
- Passwords cannot be recycled for 12 months
- Password combination – minimum of 9 characters
- Must include a capital and a number
- Authentication code added to end of the Password
- Authentication code – 1 x minute cycle only.

2. PREAMBLE

Cloud computing has become a mainstream computing service delivery alternative. According to the National Institute of Science and Technology (NIST) , cloud computing has five characteristics, and can be defined as: "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Three common service models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Use of cloud computing at MWH encompasses two main components.

1. Systems that support the business operations of Health Risk Management Systems Pty Ltd
2. Systems that support the operations of our SaaS based software, My Workplace Health by 2CRisk.

Including production services and project lifecycle environments (e.g. development, testing and production) On-demand self-service; ubiquitous network access; location transparent; resource pooling; rapid elasticity; and measured service with pay per use/ storage capabilities.

Cloud Hosting Policy and may offer benefits in the cost, performance, and delivery of IT services. The use of cloud computing services has grown and will continue to grow significantly.

3. POLICY STATEMENT

The primary reason for this policy is to facilitate a managed and co-ordinated adoption of cloud computing services by providing appropriate governance and oversight.

As the preferred option, MWH will adopt and use cloud computing services subject to business case and privacy considerations and only after issues of security and risk management have been identified and mitigated against. The total cost of ownership, with an emphasis on shifting costs from capital to approved recurring expenditure, must be taken into consideration in the procurement or adoption of all information technology and associated services. MWH's use of cloud computing services must adhere to relevant legislation associated with State and Federal information management including issues of privacy, legal, records management, and any other applicable requirements, such as, copyright, financial, ownership and geo-location of data.

The holding of data and information on externally hosted cloud computing services requires appropriate contractual agreements be in place and express authorisation for the data to be stored off site. Company data and information must not be stored in external repositories that do not have formalised or contractual agreements in place.

Any exceptions to this would require approval by the Managing Director on the recommendation of the Chief Technical Officer. Data and information stored on externally hosted cloud services remain corporate assets of MWH. These assets need to be managed appropriately, in accord with existing MWH policies. The procurement or adoption of cloud computing services, including the negotiation of contractual agreements and vendor management must be co-ordinated through the Chief Technical Officer, with approval by the Managing Director only. In the absence of the Managing Director, the Chairperson of 2CRisk Holdings Pty Ltd may take on the responsibilities of the Managing Director if required.

4. SCOPE

This policy applies to any MWH acquisition of cloud computing services and pertains to the acquisition of services from a source outside of the organisation, regardless of whether it is free or based on a subscription model. Internally hosted cloud computing services are already covered by existing process and policies. An established exception to this policy is use by the MWH authorised social media platforms that allow user content to be uploaded or modified (e.g. YouTube) without compromising our copyright guidelines, Social Media Guidelines, IT Code of Practice and using MWH information computing resources.

5. POLICY OBJECTIVES

The objectives of this Cloud Hosting Policy are to ensure:

a) Compliance with relevant legislation and policies, i.e. that the use of externally hosted services is managed in accordance with applicable State and Federal regulatory requirements and MWH Policies and guidelines.
b) An appropriate level of oversight is provided, to address the possibility of a higher level of risk existing as a result of these new service models.
c) Risks are identified, prioritised and managed in a coordinated manner.
d) Where the confidentiality, integrity, and availability of data are at risk, it is expected that the level of physical, technical, and administrative safeguards provided by the supplier are commensurate with the sensitivity and criticality of those information assets and services and match the levels of those provided in-house. Such safeguards are essential to mitigate against data breach to prevent serious harm to individuals and help protect the reputation of MWH and reduce its exposure to legal and compliance risks throughout the lifecycle of the data;
e) Effort is not duplicated (existing internal and external options should be explored prior to acquiring a new service), nor ownership of the company's assets compromised;
f) Co-ordination and appropriate interfaces exist, and that system design is in line with MWH architectural principles and standards.
g) MWH information assets remain protected and available.
h) MWH derives maximum value from expenditure on IT services.

6. RESPONSIBILITIES

The approval of the Managing Director is required prior to execution of any cloud service contracts.

7. MONITORING, REPORTING AND REVIEW

While providing benefits to MWH, implementation of cloud services can also introduce risks. As risks are identified, they must be managed through the use of an IT Risk Register. Any significant IT risks associated with hosted services must be escalated immediately to the Chief Technical Officer. The Chief Technical Officer will report regularly on the utilisation of cloud computing services and on any significant IT risks associated with hosted services, to the Managing Director

End of document.