

Security Overview

My Workplace Health Software Solutions by 2CRisk Pty Ltd

Document Identifier	Document Version	Date of Current Issue
MWH Comprehensive Security Discussion 5.1.2	2.0	16/02/2022

	Name	Role
Authored By:	R Rio	ICT Project Coordinator
Checked By:	M Cassidy	Managing Director

Version History

Version	Date	Description of Change	Authored By
1.0	16/11/2020	Initial Release	R Rio
2.0	16/02/2022	Release Update	M. Cassidy


	Name	Signature
Approved By:	M Cassidy	

Table of Contents

1: Introduction	6
1.1: Background	6
1.2: Our Solution	6
1.3: Technical Overview	7
1.4: Collection Context	7
1.5: Security Landscape Overview	7
2: Risk Management	8
2.1: Risk Management Objectives	8
2.2: Risk Management Targets	8
3: Security Policy Statement	9
3.1: Security Policy Summary	9
4: Virus Protection	10
5: Physical Security of Computer Equipment	11
5.1: Definitions	11
5.2: Categories of Risk	11
5.3: Required Physical Security	12
5.3.1 :	Security Marking 13
5.3.2 :	Locking of PC Cases 13
5.3.3 :	Sitting of Computers 13
5.3.4 :	Opening Windows 13
5.3.5 :	Blinds 13
5.3.6 :	Lockdown Devices 13
5.3.7 :	Intruder Alarm 13
5.3.8 :	Protection of Signal Transmission 13
5.3.9 :	Location of Intruder Alarms 13
5.3.10: Walk Test	13
5.3.11: Check Detectors	14
5.3.12: Anti-Masking Intruder Alarm	14
5.3.13: Break Glass Alarm Sensors	14
5.3.14: Alarm Zoning	14
5.3.15: Improved Protection of Signal Transmission	14
5.3.16: Door Specification	14
5.3.17: Intruder Alarm Sensors on Access Routes	14
5.3.18: Alarm Shunt Lock	14
5.3.19: Alarm Confirmation	14
5.3.20: Superior Protection of Signal Transmission	15
5.3.21: Improved Area Construction	15
5.3.22: External Windows to have Locks	15
5.3.23: High Risk Situations	15
5.4: Computer Room	16
6: Access Control	17
7: LAN Security	18
7.1: Hubs & Switches	18
7.2: Workstations	18
7.3: Wiring	18

7.4:	Monitoring Software	18
7.5:	Servers	18
7.6:	Electrical Security	18
7.7:	Inventory Management	18
8:	<i>Server Specific Security</i>	19
9:	<i>UNIX & Linux Specific Security</i>	20
10:	<i>Wide Area Network Security</i>	21
11:	<i>TCP/IP & Internet Security</i>	22
12:	<i>Voice System Security</i>	22
13:	<i>Acceptable Use Policy</i>	23
13.1:	User Responsibilities	23
13.2:	Electronic Mail	24
13.3:	Internet Access	25
14:	<i>Password Policy</i>	26
15:	<i>Remote Access Security Policy</i>	27
15.1:	Wireless Access	27
15.2:	Secure Access via VPN	27
15.3:	Prevention of Data Loss	27
15.4:	Remote Device Protection	27
15.5:	Bluetooth	27
15.6:	Standard Devices & Configuration	27
15.7:	Authentication	27
15.8:	Hardened Corporate Applications	27
16:	<i>Cloud Hosting: Definitions</i>	28
17:	<i>Cloud Hosting: Preamble</i>	29
18:	<i>Cloud Policy Statement</i>	30
19:	<i>Cloud Hosting Provisions</i>	31
20:	<i>Cloud Hosting Policy Objectives</i>	31
21:	<i>Cloud Hosting Responsibilities</i>	31
22:	<i>Cloud Monitoring, Reporting and Review</i>	31
23:	<i>Disaster Recovery Purpose</i>	32
24:	<i>Backups</i>	32
24.1:	The Oracle Database	32
24.1.1:	DR Native Solution	32
24.1.2:	DR AWS Solution	32
24.2:	Web Servers	32
24.3:	DNS Records	32

25:	<i>Disaster Recovery Processes</i>	33
25.1:	DR Oracle Database Process	33
25.2:	DR Web Server Process	33
25.3:	DR DNS Records	34
26:	<i>Incident Response: Availability Event & Education</i>	35
26.1:	Incident Response Procedure	35
26.2:	IR Flow Diagram	35
27:	<i>Security Event Response and Escalation</i>	36
27.1:	Security Even Procedure	36
27.2:	SE Flow Diagram	36
28:	<i>Key Areas of Support</i>	37
29:	<i>Explanation of Support</i>	37
29.1:	Support Desk Operations	38
29.2:	Incident Prioritisation and Service Levels	38
29.3:	Analysing a Service Request	39
29.4:	Closing a Service Request	39
30:	<i>Incident Management Procedure</i>	40
30.1:	Incidents Lodged by Customer: Application	40
30.1.1:	Customer System Administrator receives and validates incident	40
30.1.2:	Acceptance of the Incident	40
30.1.3:	Diagnosing the Incident	40
30.1.4:	Processing the Incident	40
30.1.5:	Closing an Incident	41
30.2:	Handling of Exceptions	41
30.2.1:	Urgent Incidents	41
30.2.2:	Functional Escalation	41
30.2.3:	Hierarchical Escalation	41
30.3:	Incidents Identified from Infrastructure Monitoring	41
30.4:	Additional Handling of Incidents involving a Security Breach	43
30.4.1:	Investigate extent of Security Breach	43
30.4.2:	Communicate with Affected Customer Representatives	43
30.4.3:	Contain the Breach:	43
30.4.4:	Investigate Source of Breach and Impact: Eradicate	43
30.4.5:	Breach Recovery	43
30.4.6:	Post Recovery Review	44
31:	<i>Threat Principles and Procedures</i>	45
32:	<i>Threat Notifications</i>	45
32.1:	Threat Notification Images	45
33:	<i>Perimeter Scans</i>	47
34:	<i>NDB</i>	47
34.1:	Process Flow	47
34.2:	NDB Responsibilities	48

35:	<i>Itoc Incident Response & Reports</i>	48
36:	<i>Database Security Model</i>	49
36.1:	Separate Database for each Customer	49
36.2:	Separate Schema for each Customer within single database	49
36.3:	2CRisk Multi-Tenanted Database	49
37:	<i>Integrated Development Environment</i>	50
37.1:	IDE: Oracle Application Express	50
37.2:	Administration System	50
37.3:	Manage Workspaces	50
37.4:	Monitor Activity & IDE Administration Password Rules	51
38:	<i>APEX Protection against External Security Threats</i>	52
38.1:	SQL Injection	52
38.2:	Cross-Site Scripting	52
38.3:	URL Tampering	52
38.4:	Eavesdropping	52
39:	<i>My Workplace Health Applications & Security</i>	53
39.1:	Company Administration	53
39.2:	Client Administration	53
39.3:	Health Risk Management	53
39.4:	Application Security Framework	53
39.5:	2CRisk Client Administration and 2cRisk Health Risk Management	53
40:	<i>Database Passwords Procedure</i>	54
41:	<i>UNIX Red Hat OS & Virtual Private Network Passwords</i>	54
42:	<i>Release Management in the SaaS Model</i>	55
42.1:	An Individual's Input on RM	55
42.2:	Prioritisation of Change	56
42.3:	Release Process	56
42.4:	Communication Points	56
42.5:	Expectation of Communication Materials	57
42.6:	Implementation Assessment Criteria	57
43:	<i>Release Management FAQ</i>	58
44:	<i>Release Management Images</i>	60

1: Introduction

2CRisk was born of a common goal to improve the health and wellbeing of the global workforce, and support organizations to implement positive change that is rewarding to both the employee and delivers positive outcomes for the business.

1.1: Background

My Workplace Health is a SaaS-based, online health risk management software solution designed, built and maintained in Australia. A 2011 and 2012 recipient of the Federal Government “Commercialization Australia” grant to develop and commercialize a software targeted at engaging primary stakeholders (employers, providers, and employees) in identifying health risks, targeting and maintaining a healthy workplace (incorporating physical and mental health).

2CRisk utilizes an Oracle cloud-based solution, operating on an EC2 Instance with Application Express (Apex) 5.1. As our software contains the electronic health records of employees, meeting the highest security and data protection is paramount and to this end, we have deployed Incapsula, DDos, Load Balancers, 256b encryption and EBS Volume encryption across of Development, Test and Production instances.

1.2: Our Solution

We aim to provide a ‘modular’ health risk management platform to employers and health providers that delivers a healthier workforce and proves the ROI in employee health, as well as to provide technology solutions to support the processes of existing providers in the provision of employment-related health assessment and services.

Our interaction with the health and wellbeing industry has led My Workplace Health to create a customisable suite of interactive software applications which enables organisations to effectively and efficiently manage their employee’s health.

From our centralised management hub *Health Cloud* clients can employ the functionality of our many satellite applications to build unique services which cater to their needs. Coined by the Greek philosopher Plato, the term ‘*Necessity is the mother of all invention*’ best describes how My Workplace Health came to exist.

The diagram below shows an overview of our currently available solutions. Visit us at <https://www.myworkplacehealth.com.au/> for further information.



2: Risk Management

My Workplace Health aims to minimise risks associated with software and web-based development. In this, we have set out the following objectives that we aim to reach every day within our practise

2.1: Risk Management Objectives

1. Ensure that risk management is clearly and consistently integrated and evidenced in the culture of MWH and our clients.
2. Manage risk in accordance with best practice
3. Anticipate and respond to changing, social, environment and legislative changes and requirements
4. Consider compliance with health and safety, insurance and legal requirements as a minimum standard
5. Prevent death, injury, damage or loss and reduce the cost of risk
6. Inform policy and operational decisions by identifying risk and their likely impact
7. Raise awareness of the need for risk management by all those connected with MWH activities and delivery of service.

2.2: Risk Management Targets

In order to meet the above objectives, My Workplace Health provides *targets and guidelines* that outline how we meet the tasks put forward.

1. Clearly defining the roles, responsibilities and reporting lines within the organisation for risk management.
2. Clearly defining and providing roles and responsibilities within MWH
3. Including risk management issues when writing reports and considering decisions
4. Consider risk management issues during monthly management meetings with clients
5. Continually demonstrating the application of risk management principals in the activities of MWH employees and member companies.
6. Reinforcing the importance of effective risk management as a part of the everyday work of employees, directors and members.
7. Maintaining a register of risks linked to MWH business activities.
8. Maintaining documented procedures for the control of risk and provision of suitable information, training and supervision.
9. Maintaining an appropriate system of recording health and safety incidents and identifying preventative measures against recurrence.
10. Preparing contingency plans to secure business continuity where there is a potential for an event to have a major impact upon the organisation's ability to function and conform to the client's requirements. These include:
 - a. Notifying clients in writing, in the event of personnel changes
 - b. Ensuring all MWH personnel have current confidentiality agreements in place
 - c. Ensuring MWH ability to maintain client contracts and to advise in writing if any financial, organisational or corporate matter changes or materially changes that may impact upon MWH ability to maintain ay contract to a high standard.
 - d. Monitor arrangements continually and seek continuous improvement.

Security Policy

3: Security Policy Statement

“It shall be the responsibility of the IT Department to provide adequate protection and confidentiality of all corporate and customer data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorised members of staff, and to ensure the integrity of all data and configuration controls.”

3.1: Security Policy Summary

- i. Confidentiality of all data is to be maintained through discretionary and mandatory access controls.
- ii. Internet and other external service access is restricted to authorised personnel only.
- iii. Access to data on all laptop computers is to be secured through encryption or other means, to provide confidentiality of data in the event of loss or theft of equipment.
- iv. Only authorised and licensed software may be installed, and installation may only be performed by IT Department staff.
- v. The use of unauthorised software is prohibited. In the event of unauthorised software being discovered it will be removed from the workstation immediately.
- vi. Data may only be transferred for the purposes determined in the Organisation’s data-protection policy.
- vii. All removable media from external sources must be virus checked before they are used within the Organisation.
- viii. Passwords must consist of a mixture of at least 9 alphanumeric characters and must be changed every 30 days and must be unique.
- ix. The physical security of computer equipment will conform to recognised loss prevention guidelines.
- x. To prevent the loss of availability of IT resources measures must be taken to backup data, applications and the configurations of all workstations.
- xi. A business continuity plan will be developed and tested on a regular basis.

4: Virus Protection

- i. The IT Department will have available up to date virus scanning software for the scanning and removal of suspected viruses. The organisation mandates the following antivirus software:
 - a. Trend Micro Security
- ii. Corporate servers will be protected with virus scanning software.
- iii. Workstations will be protected by virus scanning software. Users must not disable or remove corporate antivirus software.
- iv. All workstation and server antivirus software will be regularly updated with the latest anti-virus patches by auto update or by the IT Department.
- v. No removable media that is brought in from outside the Organisation is to be used until it has been scanned.
- vii. All removable media containing executable software (software with .EXE and .COM extensions) will be write-protected wherever possible.
- viii. All demonstrations by vendors will be run on their machines and not the Organisation's.
- ix. Only company approved and licensed software will be installed on computer systems.
 - a. Shareware is not to be used, as shareware is one of the most common infection sources. If it is absolutely necessary to use shareware it must be thoroughly scanned before use.
 - b. New commercial software will be scanned before it is installed.
- xi. All removable media brought into the Organisation by field engineers or support personnel will be scanned by the IT Department before they are used on site.
- xii. To enable data to be recovered in the event of a virus outbreak, regular backups will be carried out by the IT Department.
- xiii. Management strongly endorse the Organisation's anti-virus policies and will make the necessary resources available to implement them.
- xiv. Users will be kept informed of current procedures and policies.
- xv. Users will be notified of virus incidents.
- xvi. Employees will be accountable for any breaches of the Organisation's anti-virus policies.
- xvii. Anti-virus policies and procedures will be reviewed regularly.
- xviii. In the event of a possible virus infection the user must inform the IT Department immediately. The IT Department will then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

5: Physical Security of Computer Equipment

5.1: Definitions

Area	Two or more adjacent linked rooms which for security purposes, cannot be adequately segregated in physical terms.
Computer Room	Mainframe, minicomputer, fileserver plus all interconnected wiring, fixed disks, telecommunication equipment, ancillary, peripheral and terminal equipment linked into the mainframe, contained within a purpose-built computer room.
Computer Equipment	All computer equipment not contained within the COMPUTER ROOM which will include PC's , monitors, printers, disk drives, modems and associated and peripheral equipment.
High Risk Situation(s)	This refers to any room or AREA which is accessible <ul style="list-style-type: none"> • at ground floor level • at first floor level, but accessible from adjoining roof • at any level via external fire escapes or other features providing access • rooms in remote, concealed or hidden areas
Lockdown Device(s)	A combination of two metal plates, one for fixing to furniture, or the building structure, and the other for restraining the equipment which is immobilised when the two plates are locked together. The plate for restraining the equipment should incorporate an enclosure or other mechanism which will hinder unauthorised removal of the outer PC casing and render access to internal components difficult.
Approved	An approved security system.

5.2: Categories of Risk

Security Level 1	the security measures detailed in Level 1 are guidelines for all COMPUTER EQUIPMENT not described below.
Security Level 2	these guidelines apply where a single room or AREA contains PC's where the total replacement value of this hardware is LESS than \$20,000 per room or AREA .
Security Level 3	these guidelines apply where a single room or AREA contains PC's where the total replacement value of this hardware is between \$20,000 and \$50,000 per room or AREA .
Security Level 4	these guidelines apply where a single room or AREA contains PC's where the total replacement value of this hardware is in excess of \$50,000 per room or AREA .
Computer Room	These guidelines apply to the location or room comprising the purpose-built computer room.

5.3: Required Physical Security

The table below summarises the required features for each Security Level.

No	Security Features	Security Level			
		1	2	3	4
1	Security Marking	x	x	x	x
2	Locking of PC cases	x	x	x	x
3	Siting of computers away from windows	x	x	x	x
4	HIGH RISK SITUATION window locks	x	x	x	N/A
5	Blinds for observable windows	x	x	x	x
6	If no intruder alarm, all PC's and COMPUTER EQUIPMENT > \$1,500, to have a LOCKDOWN DEVICE	x	x	N/A	N/A
7	Intruder alarm installed by APPROVED Company		x	x	x
8	Protection of signal transmission to Alarm Receiving Centre		x	N/A	N/A
9	Assessment of location of intruder alarm protection		x	x	x
10	Walk test of movement detectors		x	x	x
11	Check that movement detectors are not obscured		x	N/A	N/A
12	Anti-masking intruder alarm sensors in room or AREA			x	N/A
13	Break glass alarm sensors			x	x
14	Individual alarm zoning of the room or AREA			x	N/A
15	Improved protection of signal transmission to Alarm Receiving Centre			x	N/A
16	Door specification for entry to room or AREA			x	x
17	Anti-masking intruder alarm sensors in room and access routes				x
18	Alarm shunt lock on door				x
19	Visual or audio alarm confirmation				x
20	Superior protection of alarm signal transmission				x
21	Improved room or AREA construction				x
22	All external opening windows to have locks				x
23	HIGH RISK SITUATION windows to have shutters/bars				x

Where an entry is shown as N/A (not applicable) this is due to a higher specification being required thereby removing the necessity for the lower security feature.

5.3.1 : Security Marking

All computer hardware should be prominently security marked by branding or etching with the name of the establishment and area postcode. Advisory signs informing that all property has been security marked should be prominently displayed externally. The following are considered inferior methods of security marking:

- Text comprised solely of initials or abbreviations
- Marking by paint or ultraviolet ink (indelible or otherwise)
- Adhesive labels that do not include an etching facility.

5.3.2 : Locking of PC Cases

PC's fitted with locking cases will be kept locked at all times.

5.3.3 : Sitting of Computers

Wherever possible, **COMPUTER EQUIPMENT** should be kept at least 1.5 metres away from external windows in **HIGH RISK SITUATIONS**.

5.3.4 : Opening Windows

All opening windows on external elevations in **HIGH RISK SITUATIONS** should be fitted with key operated locks.

5.3.5 : Blinds

All external windows to rooms containing **COMPUTER EQUIPMENT** at ground floor level or otherwise visible to the public should be fitted with window blinds or obscure filming.

5.3.6 : Lockdown Devices

For any item of **COMPUTER EQUIPMENT** with a purchase price in excess of \$1,500 which is not directly covered by an intruder alarm, the processing unit should have a **LOCKDOWN DEVICE** fitted to the workstation.

LOCKDOWN DEVICES should conform to loss prevention standards. Mobile workstations are unlikely to be suitable for these devices.

When it is impossible or undesirable to anchor hardware, such equipment can be moved to a security store or cabinet outside normal hours of occupation.

5.3.7 : Intruder Alarm

An intruder alarm incorporating the following features should be installed. Installation, maintenance and monitoring by an **APPROVED** company.

5.3.8 : Protection of Signal Transmission

Unless telephone wires directly enter the protected premises underground, signalling to the Alarm Receiving Centre should be by direct line.

5.3.9 : Location of Intruder Alarms

Detection devices should be located within the room or **AREA** and elsewhere in the premises to ensure that unauthorised access to the room or **AREA** is not possible without detection. This should include an assessment as to whether access is possible via external elevations, doors, windows and roof lights

5.3.10 : Walk Test

A walk test of movement detectors should be undertaken on a regular basis in order to ensure that all PC's are located within the alarm-protected area. This is necessary due to the

possible ongoing changes in the position of furniture, screens and partitions, which may seriously impede the field of cover provided by existing detection devices.

For any PC which is not directly covered by an intruder alarm, the processing unit should have a **LOCKDOWN DEVICE**.

5.3.11 : Check Detectors

Building managers should ensure, as part of their normal duties at locking up time, that internal space detectors have not been individually obscured or had their field of vision restricted.

5.3.12 : Anti-Masking Intruder Alarm

Anti-masking intruder alarm movement sensors are recommended to immediately detect a movement within the room or **AREA**.

5.3.13 : Break Glass Alarm Sensors

Break Glass alarm sensors to detect forced entry through external windows of the room or **AREA** are recommended.

5.3.14 : Alarm Zoning

The ability to zone the intruder alarm from the main control panel should be provided to enable authorised usage of other areas of the building outside normal hours, whilst retaining alarm detection within the room or **AREA**.

5.3.15 : Improved Protection of Signal Transmission

Unless telephone wires directly enter the protected premises underground, signalling to the Alarm Receiving Centre should be by monitored direct line.

5.3.16 : Door Specification

All doors giving access to the room or **AREA** both from within and outside the building, should be, as a minimum, solid timber and preferably unglazed. Doors should have a mortise deadlock with key registration. Door fittings should comprise 3 hinges, supplemented by 2 hinge bolts if outward opening.

Inward opening doors to the room or **AREA** should have a London bar (a metal strip strengthening the locking post of the door frame).

5.3.17 : Intruder Alarm Sensors on Access Routes

Anti-masking intruder alarm movement sensors are recommended to immediately detect a movement within the room or **AREA** and any internal corridors or rooms giving access to the room or **AREA**.

5.3.18 : Alarm Shunt Lock

The alarm should have the facility for setting within the room or **AREA** independently of the status of the main premises control panel via a shunt lock on the room or **AREA** access door. It should not be possible to set the main system if the room or **AREA** detection is 'shunted out'.

5.3.19 : Alarm Confirmation

Visual or audio alarm confirmation should be provided at the monitoring facility for all conventional detection within the room or **AREA**.

5.3.20 : Superior Protection of Signal Transmission

Monitored signalling to the Alarm Receiving Centre should be either by direct line or use monitoring service.

5.3.21 : Improved Area Construction

Secure doors giving access to the room or **AREA**, from within the building, should be solid timber and unglazed. The locking should be by 2 mortise deadlocks to with registered keys, a micro switch being available for an alarm shunt lock.

Door fittings should comprise 3 hinges, supplemented by 2 hinge bolts if outward opening doors. Inward opening doors to room or **AREA** should have a London bar (a metal strip strengthening the locking post of the door frame).

5.3.22 : External Windows to have Locks

All opening windows within the perimeter of the room or **AREA** should be fitted with key-operated window locks.

5.3.23 : High Risk Situations

Where the room or **AREA** is classified as being in a **HIGH-RISK SITUATION** the following additional protection should be provided.

Windows to external elevations should be fitted with security shutters or bars instead of locks.

Any door in the external elevation should be provided with a security shutter where practical. Considerations should be given to replacement of fire exit doors which cannot be secured in this fashion, and any other doors designated as fire escapes by the Fire Prevention Officer, with proprietary security doors and frames fitted with a four-point locking bolt and an alarm vibration sensor.

5.4: Computer Room

- i. The computer room should be housed in a purpose-built room.
- ii. In order to adequately protect the computer room and the equipment contained therein, the following activities are strictly prohibited within the computer room at any time:
 - a. Smoking
 - b. Drinking
Eating
 - c. Littering
 - d. Other inappropriate behaviour (e.g. fighting, sexual activity etc.)
- iii. The computer room should contain an adequate air conditioning system to provide a stable operating environment to reduce the risk of system crashes due to component failure
- iv. No water, rainwater or drainage pipes should run within or above the computer suite to reduce the risk of flooding.
- v. The floor within the computer room should be a raised false floor to allow computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding.
- vi. Power points should be raised from the floor to allow the smooth shutdown of computer systems in case of flooding.
- vii. Where possible generator power should provide to the computer suite to help protect the computer systems in the case of a mains power failure.
- viii. Critical systems should be connected to an uninterruptible power supply (UPS) with intelligence to cleanly shut down the computer systems on the event of mains power loss.
- ix. Access to the computer room is restricted to IT Department staff.
- x. All contractors working within the computer room are to be supervised at all times and the It Department is to be notified of their presence and provided with details of all work to be carried out, at least 48 hours in advance of its commencement.

6: Access Control

- i. Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
- ii. Users requiring access to systems must make a written application on the forms provided by the IT Department.
- iii. Where possible no one person will have full rights to any system. The IT Department will control network/server passwords and system passwords will be assigned by the system administrator in the end-user department.
- iv. The system administrator will be responsible for the maintaining the data integrity of the end-user department's data and for determining end-user access rights.
- v. Access to the network/servers and systems will be by individual username and password or certificates.
- vi. Usernames and passwords must not be shared by users.
Usernames and passwords should not be written down.
All users will have an alphanumeric password of at least 8 characters.
- vii. Passwords will expire every 90 days and must be unique. Systems shall be configured to retain a history of previous passwords where available.
- viii. Intruder detection will be implemented where possible. The user account will be locked after 3 incorrect attempts.
- ix. The IT Department will be notified of all employees leaving the Organisation's employment. The IT Department will then remove the employee's rights to all systems.
- x. Network/server supervisor passwords and system supervisor passwords will be stored in a secure location in case of an emergency or disaster, for example a fire safe in the IT Department.
- xi. Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.
- xii. IT Department staff will not login as root on to UNIX/Linux systems, but will use the *sudo/su* command to obtain root privileges.
- xiii. Use of the Administrator username on Windows is to be kept to a minimum.
- xiv. Default passwords on service software, such as databases, will be changed after installation. Where possible, the service's default username will also be changed.
- xv. On UNIX and Linux systems, rights to SSH will be restricted to IT Department staff only.
- xvi. Where possible users will not be given access to the UNIX/ Linux shell prompt.
- xvii. Access to the network/servers will be restricted to normal working hours. Users requiring access outside normal working hours must request such access in writing on the forms provided by the IT Department.
- xviii. File systems will have the maximum security implemented that is possible. Access control lists or secure file permissions must be configured across file systems.
- xix. Server backups are to be encrypted where possible. The backup media should be kept off premises to prevent complete data loss in case of physical disaster.
- xx. Access to individual customer data will only be granted with the express permission of an authorised representative of the customer. This authorisation must be received via email unless other arrangements have been expressed as part of an individual customer agreement,

7: LAN Security

7.1: Hubs & Switches

LAN equipment, hubs, bridges, repeaters, routers, switches will be kept in secure hub rooms. Hub rooms will be kept locked at all times. Access to hub rooms will be restricted to IT Department staff only.

Other staff and contractors requiring access to hub rooms will notify the IT Department in advance so that the necessary supervision can be arranged. LAN equipment passwords must be changed from defaults.

7.2: Workstations

Users must logout of their workstations when they leave their workstation for any length of time. Alternatively, Windows workstations may be locked.

All unused workstations must be switched off outside working hours.

7.3: Wiring

- a. All network wiring will be fully documented.
- b. All unused network points will be de-activated when not in use.
- c. All network cables will be periodically scanned, and readings recorded for future reference.
- d. Users must not place or store any item on top of network cabling.
- e. Redundant cabling schemes will be used where possible.

7.4: Monitoring Software

- a. The use of LAN analyser and packet sniffing software is restricted to the IT Department.
- b. LAN analysers and packet sniffers will be securely locked up when not in use.
- c. Intrusion detection systems will be implemented to detect unauthorised access to the network

7.5: Servers

All servers will be kept securely under lock and key. All physical servers are kept off site in a secure location, and all cloud servers are restricted to authorised IT Department staff only.

7.6: Electrical Security

- a. All servers will be fitted with UPS's that also condition the power supply.
- b. All hubs, bridges, repeaters, routers, switches and other critical network equipment will also be fitted with UPS's.
- c. In the event of a mains power failure, the UPS's will have sufficient power to keep the network and servers running until the generator takes over.
- d. Software will be installed on all servers to implement an orderly shutdown in the event of a total power failure.
- e. All UPS's will be tested periodically.

7.7: Inventory Management

- a. The IT Department will keep a full inventory of all computer equipment and software in use throughout the Company.
- b. Computer hardware and software audits will be carried out periodically via the use of a desktop inventory package. These audits will be used to track unauthorised copies of software and unauthorised changes to configurations

8: Server Specific Security

This section applies to the organisation's servers:

- i. The operating system will be kept up to date and patched on a regular basis. Servers will be checked daily for viruses.
Servers will be locked in a secure room.
Where appropriate the server console feature will be activated.
- ii. Remote management passwords will be different to the Admin/Administrator/root password.
- iii. Users possessing Admin/Administrator/root rights will be limited to trained members of the IT Department staff only.
- iv. Use of the Admin/Administrator/root accounts will be kept to a minimum.
- v. Assigning security equivalences that give one user the same access rights as another user will be avoided where possible.
- vi. User access to data and applications will be limited by the access control features.
- vii. Intruder detection and lockout will be enabled. The system auditing facilities will be enabled.
- viii. Users must logout or lock their workstations when they leave their workstation for any length of time.
- ix. All unused workstations must be switched off outside working hours.
- x. All accounts will be assigned a password of a minimum of 8 characters.
- xi. Administrative users will change their passwords every 45 days.
- xii. Unique passwords will be used.
- xiii. The number of grace logins will be limited to 3.
- xiv. The number of concurrent connections will be limited to 1.
- xv. Network login time restrictions will be enforced preventing users from logging in to the network outside normal working hours.
- xvi. In certain areas users will be restricted to logging in to specified workstations only.

9: UNIX & Linux Specific Security

- i. Direct *root* access will be limited to the system console only. Administrators must still login with their credentials to the server.
- ii. IT Department staff requiring root access must make use of the sudo command (su where sudo is not available).
- iii. Use of the root account will be kept to a minimum.
- iv. All daemon accounts must not have shell logins.
- v. Insecure services, those which do have encryption or commonly have vulnerabilities, must be disabled unless there is no alternative. Where these services are to be active, access to them must be within an isolated network with additional security provision, such as an administrative Virtual LAN. Insecure services include:
 - a. FTP
 - b. Telnet
 - c. rlogin
 - d. rsh
 - e. VNC
 - f. X11
- vi. SSH facilities will be restricted to authorised users.
- vii. User access to data and applications will be limited by the access control features.
- viii. Users will not have access to the command line shell.
All account passwords must adhere to the Password Policy. Users will change their passwords every 45 days.

10: Wide Area Network Security

- i. Wireless LANs will make use of the most secure encryption and authentication facilities available.
- ii. Users will not install their own wireless equipment under any circumstances.
- iii. Dial-in modems will not be used if at all possible. If a modem must be used dial-back modems should be used. A secure VPN tunnel is the preferred option.
- iv. Modems will not be used by users without first notifying the IT Department and obtaining their approval.
- v. Where dial-in modems are used, the modem will be unplugged from the telephone network and the access software disabled when not in use.
- vi. Modems will only be used where necessary; in normal circumstances all communications should pass through the Organisation's router and firewall.
- vii. All bridges, routers and gateways will be kept locked up in secure areas.
- viii. Unnecessary protocols will be removed from routers.
- ix. The preferred method of connection to outside Organisations is by a secure VPN connection, using IPSEC or SSL.
- x. All connections made to the Organisation's network by outside organisations will be logged.

11: TCP/IP & Internet Security

- i. Permanent connections to the Internet will be via the means of a firewall to regulate network traffic.
- ii. Permanent connections to other external networks, for offsite processing etc., will be via the means of a firewall to regulate network traffic.
- iii. Where firewalls are used, a dual homed firewall (a device with more than one TCP/IP address) will be the preferred solution.
- iv. Network equipment will be configured to close inactive sessions.
- v. Where modem pools or remote access servers are used, these will be situated on the DMZ or non-secure network side of the firewall.
- vi. Workstation access to the Internet will be via the Organisation's proxy server and website content scanner.
- vii. All incoming e-mail will be scanned by the Organisation's e-mail content scanner.

12: Voice System Security

- i. The maintenance port on the PBX will be protected with a secure password.
- ii. The default and maintenance passwords on the PBX will be changed to user defined passwords.
- iii. Internal and external call forwarding privileges will be separated, to prevent inbound calls being forwarded to an outside line.
- iv. The operator will endeavour to ensure that an outside call is not transferred to an outside line.
- v. Use will be made of multilevel passwords and access authentication where available on the PBX.
- vi. Voice mail accounts will use a password with a minimum length of six digits.
- vii. The voice mail password should never match the last six digits of the phone number.
- viii. The caller to a voice mail account will be locked out after three attempts at password validation.
- ix. Dialling calling party pays numbers will be prevented.
- x. Telephone bills will be checked carefully to identify any misuse of the telephone system.

13: Acceptable Use Policy

13.1: User Responsibilities

These guidelines are intended to help you make the best use of the computer resources at your disposal. You should understand the following.

- i. You are individually responsible for protecting the data and information in your hands. Security is everyone's responsibility.
- ii. Recognise which data is sensitive. If you do not know or are not sure, ask.
- iii. All customer data is deemed to be sensitive
- iv. No customer data is to be exported to a localised or external drive without the express permission of an authorised customer representative
- v. No customer data is to be exported to a flat file without the express permission of an authorised customer representative
- vi. No customer data is to be emailed to another person including employees or external parties
- vii. Even though you cannot touch it, information is an asset, sometimes a priceless asset.
- viii. Use the resources at your disposal only for the benefit of the Organisation.
 - a. Understand that you are accountable for what you do on the system. If you observe anything unusual, tell your supervisor.

When using the Organisation's computer systems, you should comply with the following guidelines.

DO

- xi. Do choose a password that is hard to guess; refer to the Password Policy for guidance.
- xii. Do log off or lock your PC before you leave your workstation. This is important if you are working on sensitive information or leaving your workstation for any length of time.
- xiii. Do ask people their business in your area, if they look as though they do not belong there.
- xiv. Do protect equipment from theft and keep it away from food and drinks.
- xv. Do ensure that all important data is backed up regularly. Liaise with the IT Department if you require assistance.
- xvi. Do make sure that on every occasion external hard disks, CD's, DVD's and USB sticks are brought in to the Organisation that they are checked for viruses before use.
- xvii. Do inform the IT Department immediately if you think that your workstation may have a virus.

DO NOT

- xviii. Do not write down your password.
- xix. Do not share or disclose your password.
- xx. Do not give others the opportunity to look over your shoulder if you are working on something sensitive.
- xxi. Do not use shareware (software downloaded from the Internet or on PC magazine covers).
- xxii. Do not duplicate, copy or distribute software.
- xxiii. Do not install any software on your machine or alter its configuration, this work may only be undertaken by the IT Department.
- xxiv. Do not export and share customer data

Please Note the following:

- Your PC will be audited periodically.
- Logins to and use of the Organisation's network are monitored and audited.

Failure to comply with the organisation's security policy may lead to disciplinary action.

13.2: Electronic Mail

These guidelines are intended to help you make the best use of the electronic mail facilities at your disposal.

The Organisation provides electronic mail to staff to enable them to communicate effectively and efficiently with other members of staff, other companies and partner organisations.

When using the Organisation's electronic mail facilities, you should comply with the following guidelines.

DO

- Do check your electronic mail daily to see if you have any messages.
- Do include a meaningful subject line in your message.
- Do check the address line before sending a message and check you are sending it to the right person.
- Do delete electronic mail messages when they are no longer required.
- Do respect the legal protections to data and software provided by copyright and licenses.
- Do take care not to express views, which could be regarded as defamatory or libellous.

DO NOT

- Do not print electronic mail messages unless absolutely necessary.
- Do not expect an immediate reply, the recipient might not be at their computer or could be too busy to reply straight away.
- Do not forward electronic mail messages sent to you personally to others, particularly newsgroups or mailing lists, without the permission of the originator.
- Do not participate in chain or pyramid messages or similar schemes.
 - Do not represent yourself as another person.
- Do not use electronic mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive or libellous.

Please Note the following:

- All electronic mail coming into or leaving the Organisation is scanned for viruses.
- All the content of electronic mail is scanned for offensive material.

If you are in any doubt about an issue affecting the use of electronic mail you should consult the IT Department.

Any breach of the Organisation's Electronic Mail Acceptable Use Policy may lead to disciplinary action.

13.3: Internet Access

These guidelines are intended to help you make the best use of the Internet resources at your disposal. You should understand the following.

- The Organisation provides Internet access to staff to assist them in carrying out their duties for the Company. It is envisaged that for the majority of the working time, it will be used to enable you to execute your role effectively,
- The Internet may be used for personal circumstances and expects that use will be in line with company values
- You may only access the Internet by using the Organisation's content scanning software, firewall and router.

When using the Organisation's Internet access facilities, you should comply with the following guidelines.

DO

- i. Do check that any information you access on the Internet is accurate, complete and current.
- ii. Do check the validity of the information found.
- iii. Do respect the legal protections to data and software provided by copyright and licenses.
- iv. Do inform the IT Department immediately of any unusual occurrence.

DO NOT

- i. Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
- ii. Do not download software from the Internet and install it upon the Organisation's computer equipment.
- vii. Do not use the Organisation's computers to make unauthorised entry into any other computer or network.
- iii. Do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse Act 1990.
- iv. Do not represent yourself as another person.
- v. Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.

Please note the following

- All material viewed is scanned for viruses.
- All the content viewed is scanned for offensive material.

If you are in any doubt about an issue affecting Internet Access, you should consult the IT Department.

Any breach of the Organisation's Internet Acceptable Use Policy may lead to disciplinary action.

14: Password Policy

In order to make it harder for people to guess your passwords please keep in mind the following advice:

- i. **Don't use dictionary words** - All real words are easy to guess. Avoid using any words, words in foreign languages, swear words, slang, names, nicknames, etc.
- ii. The names of family, friends and partners, anniversary dates, car registrations and telephone numbers are the first thing potential crackers will try when guessing your passwords.
- iii. Instead try to **pick acronyms, mnemonics, random letters**, etc, or **insert nonalphabetic characters in the middle of the word, replace letters with numbers** ('o' to zero, l to 1, E to 3), etc.
- iv. Use a mIxTuRe of UPPER and lower case on case sensitive systems - Unix and Linux.
- v. You must **include a number** (0-9) somewhere in the password. Try to fit this in somewhere inside whatever letters you choose, instead of at the end or beginning of the password.
- vi. If possible, **include a symbol** (£\$%&^*+=) somewhere in the password.
- vii. When changing passwords, **change more than just the number**: perhaps move its position within the password, add or subtract letters, change capitalisation, etc.
- viii. However, **choose something you can remember**. This is very important; it is no good having a password like "h498cj3t34" if you have it written on a PostIt Note stuck to your monitor! If you must have a reminder or hint, use something cryptic that only you can understand.
- ix. **Never tell anyone else your password or allow them to log in as you**. Avoid telling anyone your password on the telephone, hackers often ring up pretending to be from the Information Technology Department and ask for your password. If it is necessary to provide your password to someone else to allow a fault to be fixed, ensure that they are genuine members of Information Technology Department first with physical identification.
- x. Try to avoid letting other people watch you key your password in. Choose something that is not easy to guess from watching, like "qwerty12345".

15: Remote Access Security Policy

15.1 : Wireless Access

Where the network is accessed remotely via wireless appropriate wireless security standards will be used. Wi-Fi Protected Access II (WPA2) will be used as standard on Wi-Fi connections. A WPA2 encryption key will be used. The network will be configured not to advertise its presence.

The power of access points will be turned down to a minimum that still allows the access point to function. Due to the possibility of cracking Wireless Encryption Protocol using sniffing software such as AirSnort all wireless access points will be outside the firewall.

15.2 : Secure Access via VPN

Access from remote users to the corporate network will be via secure IPSEC VPN or SSL VPN connections only. This is necessary to secure the connection from the remote device to the corporate network.

15.3 : Prevention of Data Loss

All laptops and PDA's that are taken off site will have the following security configured, to prevent data loss in the event of theft. The hardware password will be enabled if available. Sensitive documents will be accessed remotely and not downloaded to the laptop or PDA.

15.4 : Remote Device Protection

To prevent remote PC's, laptops, PDA's etc from compromising the corporate network, security software will be installed on the devices. Firewall software will be installed on the devices to prevent them from being compromised by trojans and back door software. Anti-virus software configured to automatically download the latest virus signatures will be installed and utilised.

15.5 : Bluetooth

To prevent Bluetooth enabled devices from being attacked and compromised the Bluetooth connections on mobile phones, PDA's and laptops will be disabled where appropriate. This is to prevent bluejacking, SNARF and backdoor attacks.

15.6 : Standard Devices & Configuration

Devices that are used to access the network remotely, must meet the minimum standard for supported web browsers and operating systems that is current at the time of access. Where access is provided directly to the corporate network, users will only be allowed access on standard devices authorised and approved by corporate ICT Services.

15.7 : Authentication

Authentication for remote access will use two-stage authentication. As a minimum this will comprise two-stage username and password verification. Where possible to enhance the authentication of users one of the following additional methods of authentication will be used in conjunction with the user's password.

- Digital Certificate
- Smart Card
- SecureID Card

15.8 : Hardened Corporate Applications

All corporate applications will be hardened as much as possible, particular attention will be paid to those applications, which are accessible remotely. The security features of applications will be fully utilised, and all security patches will be applied.

Security Policy: Cloud Hosting

16: Cloud Hosting: 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
 - c. Development Environment
 - i. Test Environment
 - ii. Production Environment
 - d. Amazon Web Services (AW) hosting
 - e. APEX Environment (Application Express)
 - f. Imperva Cloud Security platform
- c. 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.

17: Cloud Hosting: 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.

18: Cloud 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.

19: Cloud Hosting Provisions

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.

20: Cloud Hosting 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.

21: Cloud Hosting Responsibilities

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

22: Cloud 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

Disaster Recover Procedures

23: Disaster Recovery Purpose

This document has been prepared for My Workplace Health to provide the current disaster recovery procedures of the platform. The following items are in scope for this document:

- Backup procedures of the My Workplace Health environment
- Recovery procedures of the My Workplace Health environment

24: Backups

The following processes are required to achieve the desired customer outcomes

24.1: The Oracle Database

There are two backup solutions deployed for the Oracle Database: a native oracle solution and an AWS solution.

24.1.1: DR Native Solution

The first backup solution is a native oracle solution on the Database server. This solution utilises Oracle's Recovery Manager (RMAN) to perform backups and recovery tasks on the database. The RMAN backups occur nightly at 1am AEST and retained for 7 days. The RMAN backups are stored in Oracle's Flash Recovery Area in the file *db_recovery_file_dest* located in */data/app/oracle/fast_recovery_area/*.

To perform the RMAN backups, a cron job has been configured to run the following shell script.

```
#!/bin/sh
rman target=/ @/data/scripts/rman_script.txt
```

The shell script initiates the RMAN job by targeting a file containing the following RMAN commands.

```
RUN {
REPORT SCHEMA;
CROSSCHECK
BACKUP;
CROSSCHECK ARCHIVELOG ALL; BACKUP DATABASE
PLUS ARCHIVELOG; DELETE OBSOLETE;
```

24.1.2: DR AWS Solution

The AWS solution has been deployed alongside and takes snapshots of the EBS volumes attached to the Database every 15 minutes. These snapshots are retained for 7 days

24.2: Web Servers

For the web servers, the AWS solution has been deployed. This solution takes snapshots of the EBS volumes daily at 3.00am AEST. These snapshots are retained for 7 days.

24.3: DNS Records

DNS backups are taken of the full Route 53 record set in My Workplace Health's AWS account. These are completed by using Itoc's customer Route 53 backup solution which

takes the backups using a Lambda Function triggered by a CloudWatch event to occur at 5.00pm AEST. When the function is triggered a full backup of each hosted zone is recorded to a text file and upload to S3 as a zip file. These are retained forever.

25: Disaster Recovery Processes

The recovery process depends on the scenario however the below documents outline the standard recovery procedures for the environment.

25.1 : DR Oracle Database Process

The below steps would be completed in order to recover the Oracle Database. These should be completed in order and proceeded to the next section only if the above fails.

1. Restore server availability:
2. SSH onto the instance
3. Confirm the Oracle Listener is up
 - i. If not running start the Listener
4. confirm the database status is active and open
5. Ensure the hostname of the server is *prod-database.aws.2crisk.net*
2. Restore and Recover using Oracle RMAN
6. SSH onto the instance and become the Database user.
7. Perform the below command if only a media recovery is required
8. RECOVER DATABASE;
 - i. Perform the below command if a complete restoration is required:
9. RESTORE DATABASE;
10. RMAN> RECOVER DATABASE;
11. Restore EBS volumes if missing or corrupted:
 - i. Using the latest snapshot of the target volume create a new volume.
 - ii. Stop the instance
 - iii. If applicable, unattach the volume from the instance, recording the mount point
 - iv. Attached the newly created volume to the instances
 - v. Start instance
 - vi. SSH onto the instance to confirm data is present
 - vii. Confirm running process and endpoints.
12. If the above fails, Itoc Managed Services will escalate to a Database Administrator within the company.

25.2 : DR Web Server Process

The following steps would be completed if the Web Servers need restoring. These should be completed in order and proceeded to the next section only if the above fails.

1. Restore server availability:
 - a. SSH onto the instance
 - b. Confirm NGINX is running
 - c. If not running start the NGINX server
2. Restore EBS volumes if missing or corrupted:
 - a. Using the latest snapshot of the target volume create a new volume.
 - b. Stop the instance
 - c. If applicable, unattach the volume from the instance, recording the mount point
 - d. Attached the newly created volume to the instances
 - e. Start instance
 - f. SSH onto the instance to confirm data is present
 - g. Confirm running process and endpoints.

25.3: DR DNS Records

The following steps would be completed if the DNS records need to be restoring:

1. Navigate to S3 in My Workplace Health's AWS account
2. Select the S3 bucket retaining all DNS backups
3. Download the zip file of the hosted zone that you wish to restore the records to
4. Update the Route53 Hosted Zone record set with the backup record set
5. Confirm desired endpoints are reachable.

Incident Response Procedures

26: Incident Response: Availability Event & Education

26.1: Incident Response Procedure

In the event that an issue causes a component of the platform to either become unavailable or enter a degraded state such that 2CRisk's application is impacted, Itoc staff are notified via the PagerDuty alerting system. For those components that are monitored, please refer to Application Level Monitoring & Metrics, Standard Host Level Monitoring & Metrics and Web Checks, Monitoring & Metrics in the 2CRisk Operations Guide.

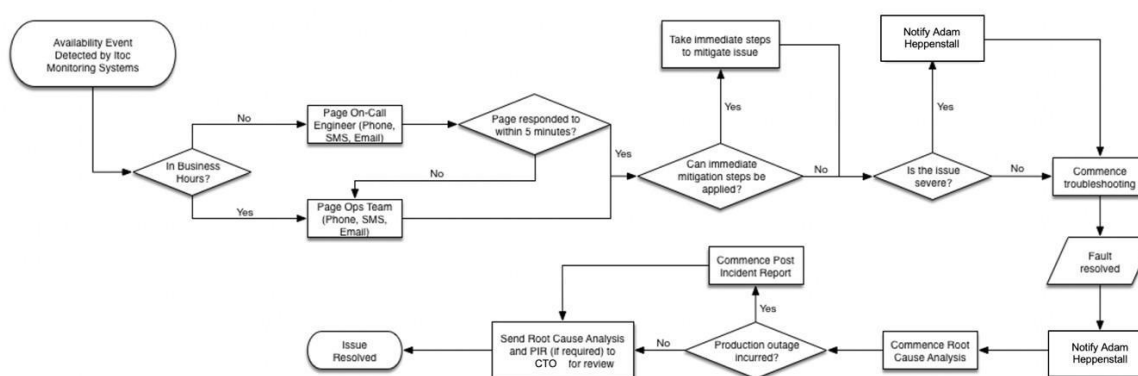
The PagerDuty alerting system is operational and actively monitored by the Cloud Ops Team during business hours, and by the On-Call Engineer outside operating hours. Escalation paths are configured to alert all members of the Cloud Ops Team if the On-Call Engineer does not respond within 5 minutes of the alert.

The engineer assigned to the alert will then assess the degree of severity of the event. If there is an immediate response that can be applied in order to resolve the alert, such as rebooting a server that has crashed due to running out of memory, the engineer will follow this procedure.

In the event that more detailed troubleshooting is required to determine the root cause of the fault and the path to resolution, the engineer will notify Adam Heppenstall at 2CRisk of the issue and estimated resolution time. If the estimated resolution time is unknown, the engineer will arrange a plan to contact Adam Heppenstall at intervals until the issue is resolved to ensure that he is kept up to date on the status.

Following the resolution of the issue, the engineer will update 2CRisk, and then commence the root cause analysis. In the event that there was an outage to the Production system as a result of the issue, the engineer will also begin a Post Incident Report (PIR). The PIR will contain the root cause analysis, the resolution steps and any recommendations to avoid the fault in future, if applicable, and will be sent to Adam Heppenstall upon completion.

26.2: IR Flow Diagram



27: Security Event Response and Escalation

27.1: Security Even Procedure

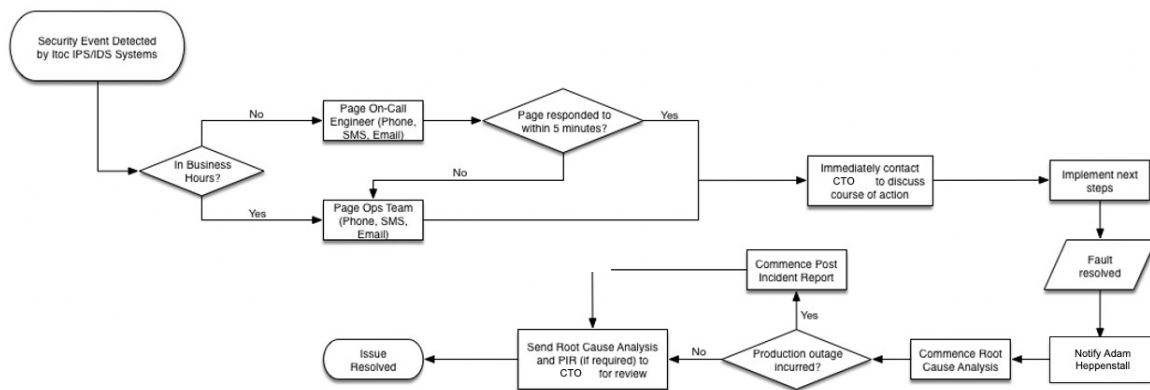
If the event of a security issue where a component of the platform has been compromised in some way (e.g. virus/malware infection, unauthorized access event, unexpected binary file modification, etc) that triggers Itoc's Trend Micro IPS/IDS system, the PagerDuty alerting system notifies Itoc staff immediately upon detection.

The PagerDuty alerting system is operational and actively monitored by the Cloud Ops Team during business hours, and by the On-Call Engineer outside operating hours. Escalation paths are configured to alert all members of the Cloud Ops Team if the On-Call Engineer does not respond within 5 minutes of the alert.

The engineer assigned to the alert will immediately notify Adam Heppenstall at 2CRisk of the issue, and the details provided by the IPS/IDS system. Appropriate next steps will be determined and implemented, such as terminating the compromised resource or restricting the resource's outbound traffic and redirecting all 2CRisk traffic to a maintenance page until the scope of the event and steps to resolution have been agreed upon.

Following the resolution of the issue, the engineer will update 2CRisk and then commence the root cause analysis and a Post Incident Report (PIR). The PIR will contain the root cause analysis, the resolution steps and any recommendations to avoid the fault in future, if applicable, and will be sent to Adam Heppenstall upon completion.

27.2: SE Flow Diagram



Our Service Standards

28: Key Areas of Support

My Workplace Health is a cloud-based application and every effort has been made in the design of the software and corresponding implementation approach to enable our Customers to be self-sufficient in the day to day operation of the software.

Our ongoing approach to providing effective support and service to our Customers covers **five key areas:**

1. Providing Support to:
 - a. Build User Competence
 - b. Resolve Incidents reported by the User
2. Correcting identified 'bugs' in the software
3. Assuring continuity of Customer Processes and Operations
4. Obtaining Customer requests for new or enhanced capability
5. Developing, testing and Releasing new capability

This document focuses on the availability of Support to our Customers and the Service Level Agreement and process to resolve any incident.

29: Explanation of Support

MWH provides support via its Support Desk and associated staff, located in Melbourne.

Support is provided on the following basis and is included as a part of the Subscription Fee:

- 10x 5 support (in reality, we support you when you need it)
- Access to all upgrades and new functionality with the relevant applications selected
- Maintenance
- All IT infrastructures (server & storage)
- Back up and Disaster Recovery

The Support staff provides a range of skills including technical, process and functional and our philosophy is to go the extra mile to ensure customer satisfaction is maintained at least and all efforts made to exceed customer expectations.

MWH recognizes that as a cloud provider we have *3 key obligations* as part of our contracts:

1. To assure wherever possible that MWH functions as advertised
2. That customer data is protected and secure
3. That customer business process continuity is maintained
4. That the performance of the infrastructure delivers acceptable performance

Zoom Conference

MWH also offers client the use of the ZOOM Conference system, viewable on the system dashboard as an Icon with a direct link to the on-duty support officer via email.

A secure link and SMS code is sent to the user, whereby screen share and a voice link are achieved. Please note that this service can be added to existing clients at an initial implementation costs and then an hourly rate for assistance provided deemed to be outside the scope of normal system support.

29.1 : Support Desk Operations

The Support Desk operates on a 10 x 5, Monday to Friday from 08:00 to 18:00 AEST.

Outside of these standard business hours, MWH maintains an on-call system for **Urgent** calls which are impacting on Customer business operations. Low, Medium and High priority calls received outside of these hours will be recorded and actioned the next business day.

Urgent Incidents can be recorded by calling the MWH Support toll free support number **1300 736 361**.

Please Note:

The afterhours support service is only contactable through the toll-free number All calls logged through email will be addressed during the next business day.

All non-urgent incidents and service requests logged after standard business hours will be addressed during the next business day.

The objective for afterhours support is to restore the affected services as soon as possible. The respective Incident records will be recorded the next business day, including any root cause analysis and reporting

Support requests can be lodged via email or phone:

- Phone: 1300 736 361
- Email: support@2crisk.com.au

The **1300 736 361** toll free number is directed to an individual member of the service desk hunt group. All service desk personnel have their phone extensions and / or mobiles placed in this group.

For non-urgent incidents, the support@2crisk.com.au email address is the preferred method for reporting an incident. This address is pointed to key support personnel and is coordinated by the Support Manager to ensure coordinated response.

29.2 : Incident Prioritisation and Service Levels

Service Request Prioritisation	Definition	Target Response Time	Target Resolution Time
Low	The incident does not require immediate attention, and there is little or no impact on business processes	7 days	30 days
Medium	Users can perform day to day tasks and a workaround is available. There is little impact to business process, but it is causing a slight inconvenience	24 hours	7 days
High	Users cannot perform day to day tasks in a sustainable way, and a work around may not be available. Productive user of the system is possible, however, will impact on the business in the very near term	2 hours	1 day
Urgent	Impacts significantly on business operations, and productive use of the system is not possible. There is no workaround available.	1 hour	Same Day

29.3: Analysing a Service Request

The MWH support consultant will perform a detailed analysis of the service request, providing documented information to the Customer representative of the solution.

29.4: Closing a Service Request

MWH Service Desk will only close a service request once a suitable solution has been provided and the Customer representative has reviewed and confirmed call closure.

30: Incident Management Procedure

Incident management is the process responsible for managing the lifecycle of all incidents. The primary objective of incident management is to restore the MWH service to end users as quickly as possible.

The process detailed below details the 'typical' incident management procedure. It assumes that a System Administrator has been trained for each Customer to provide **Level 1 Support** to their end users.

As part of any implementation process, the agreed incident reporting and management process is tailored to meet Customer need and can include Level 1 support being provided by the MWH Support Team.

30.1 : Incidents Lodged by Customer: Application

30.1.1 : Customer System Administrator receives and validates incident
To increase the reliability and effectiveness of the Incident Management process, end users are encouraged to report incidents to the Customer System Administrator. The Customer System Administrator validates the incident to ensure that the end user has provided the minimum information needed to resolve the incident.

The Customer System Administrator will resolve the incident if able to. If not, the incident is escalated to the MWH Support Team for further analysis and investigation.

30.1.2 : Acceptance of the Incident
The MWH Service Desk acknowledges receipt of call by means of contacting the Customer System Administrator and confirms acceptance of the incident.

The MWH service desk consultant will ensure that the incident is assigned to the best, available consultant to investigate the incident, based on the impact and urgent provided by the Customer System Administrator.

30.1.3 : Diagnosing the Incident
The MWH consultant works closely with the Customer System Administrator on determining the nature of the incident. This may involve more detailed discussions between the MWH consultant, the Customer System Administrator and possibly the end user. Any agreed actions will be distributed by the MWH consultant, by email to all stakeholders (including Customer System Administrator and MWH Service Desk).

The consultant will attempt to recreate the incident in the MWH Test client or seek permission to access the Customer live environment for further investigation if the incident can't be reproduced in the MWH Test client.

30.1.4 : Processing the Incident
During the investigation of the incident, the MWH consultant may require further information to assist with the diagnosis. All information received from the Customer System Administrator will be attached to the incident record. In the event that the incident needs to be escalated to another consultant, the MWH Service Desk will transfer all actions performed thus far as well as any attachments.

Once a workaround has been identified, the consultant will document the resolution and provide details to the Customer System Administrator.

30.1.5 : Closing an Incident

MWH Service Desk will only close an incident once a workaround has been provided and the Customer System Administrator has reviewed and confirmed call closure. In the event that the incident reoccurs, a new incident will be lodged, and a problem record created to investigate the root cause of the reoccurring Incidents. MWH will provide, implement and communicate the incident management process to be adopted by MWH, for review by the Customer.

30.2: Handling of Exceptions

30.2.1 : Urgent Incidents

These are critical incidents that require a response above and beyond that provided by the normal incident process. Such incidents may have a major impact on the ability to sustain operations or effectively run the business. Although these incidents still follow the normal incident life cycle, increased coordination, escalation, communication, and resources will be applied in these instances appropriate for high-severity events.

To ensure continuous work and focus on Urgent incident, MWH will require the Customer System Administrator to be available to provide documentation and assistance.

The MWH Service Desk Manager (or appropriate delegate) is responsible for ensuring clear, consistent communication to the Customer System Administrator during the lifecycle of a major incident.

All Urgent incidents will result in a *problem root cause analysis*.

30.2.2 : Functional Escalation

In the event that MWH are not able to resolve the incident within the SLA resolution timeframe, the MWH consultant will escalate the incident to another support consultant within the MWH team.

30.2.3 : Hierarchical Escalation

A hierarchical escalation is needed when Customer logs a major Incident or requests an existing incident is raised to Urgent severity (either due to impact or urgency to the organisation).

The MWH Service Desk will ensure that the Service Desk manager is notified of the hierarchical escalation. The MWH Service Desk Manager (or appropriate delegate) is responsible for ensuring clear, consistent communication to the Customer System Administrator during the lifecycle of a major incident.

30.3: Incidents Identified from Infrastructure Monitoring

MWH is hosted on infrastructure provided by Amazon Web Services and managed by an outsourced Managed Service Provider, ITOC Australia.

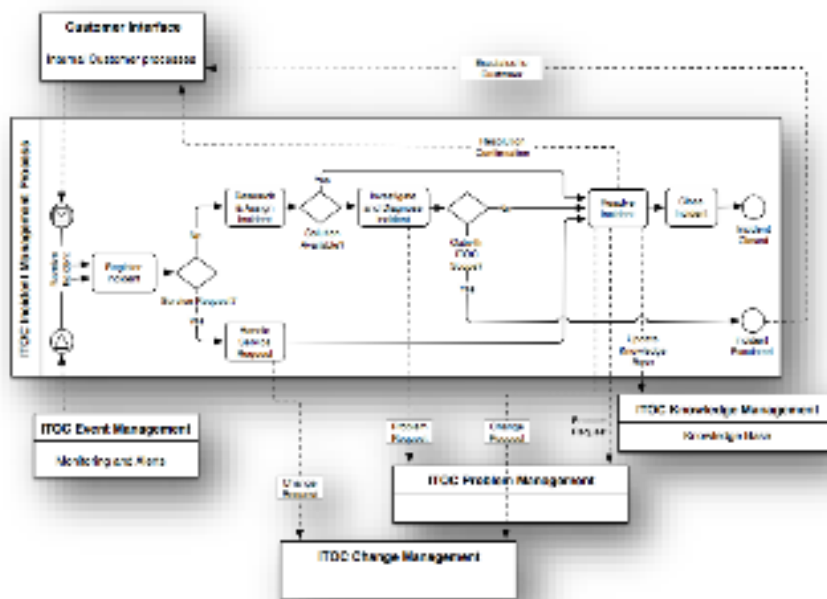
ITOC Australia has responsibility for the monitoring of availability and performance of the servers including maintenance at operating system and database levels

MWH is a cloud-based application and as such, ITOC also provide monitoring for external threats that may impact on Security

For any incident arising as the result of monitoring the Infrastructure hosted at Amazon Web Services and managed by ITOC Australia:

1. For all critical alerts which have the potential to impact on the operation of MWH, the ITOC Support Consultant addresses the alert to identify a possible workaround and mitigate the risk to MWH and its Customers.
Please Note: All critical alerts will be raised with a severity of Urgent depending on the impact to MWH Customers and urgency to find a suitable workaround.
2. ITOC will alert the MWH Support Team Manager in the event of detecting a critical alert and determine the impact on the Customers and likely timeframe for resolution
3. The MWH Support Team Manager will contact all Customer System Administrators via email to alert them to the impact and likely timescale for resolution
4. The MWH Support Team Manager will maintain regular communication with the ITOC Service Desk and update the Customer System Administrators via email as necessary
5. Following resolution of the incident, the MWH Support Team Manager immediately notifies the Customer System Administrators detailing the critical alert and the actions taken to mitigate the risk.

The ITOC internal Incident Management Process is described in the *process flow below*



30.4 : Additional Handling of Incidents involving a Security Breach

MWH stores personal and health related data and as such, take every precaution to minimize the risk of unauthorized access to the data it maintains on its Customers behalf. The proactive steps taken to minimize these risks are described in the document HRMS Systems Security Model and the MWH Security Overview document.

Should unauthorized access to customer data be detected, the incident management process described previously will be followed and all security related incidents will be classified as an Urgent Incident.

The additional communication and investigation steps described below will be initiated to ensure Containment, Eradication and Recovery process is followed.

As with the other phases of Incident Response, close coordination with all stakeholders is required to ensure that strategies developed to contain, eradicate, and recover from an incident are effective, efficient, and take into consideration all legal and privacy implications.

In the event of a security breach, the following additional steps will be initiated, and the appropriate course of action determined with all key stakeholder's dependent on the nature and extent of the security breach.

30.4.1 : Investigate extent of Security Breach

- a. Does the security breach affect one Customer or multiple Customers?
- b. Was the security breach detected by one Customer and the root cause clearly identified as the result of a malicious internal attack leading to corruption or distribution of data by an end user of that Customer?

30.4.2 : Communicate with Affected Customer Representatives

- a. Describe the nature and extent of the breach and recommended course of action
- b. Determine communication strategy to be taken by MWH and Customer(s) to the affected stakeholders
- c. Affected stakeholders could include Employer, Unions, Government Agencies, Service Providers and individual employees whose data has been accessed, corrupted or distributed

30.4.3 : Contain the Breach:

- a. If isolated to a single customer – remove access to all users for that Customer
- b. If system wide breach – block access to MWH at the Elastic Load Balancer in the AWS environment

30.4.4 : Investigate Source of Breach and Impact: Eradicate

- a. Investigate root cause of breach
- b. Determine corrective actions to eradicate / minimize risk of similar breach in the future

30.4.5 : Breach Recovery

- a. Recovery efforts include robust verification that the root cause has been identified and remediated prior to MWH coming back on-line. This is crucial to avoiding a "race condition" where an un-identified vulnerability allows the attacker to compromise newly provisioned instances. This may require recreating a base image or restoring a known good backup and applying the mitigation. For attacks targeted lower in the stack, MWH will verify that any configuration errors, patches, or other remediation efforts have been universally deployed. The following Recovery steps will be initiated:

- b. Define recovery plan: This will always include implementation of corrective actions determined as part of the Eradication step
- c. Recovery options include restoration of data from back-up taken prior to breach for affected Customer(s) or creation of a new instance of MWH
- d. Communicate investigation, findings, eradication steps and recommended recovery plan to affected Customer Representatives
- e. Implement Recovery Plan

30.4.6 : Post Recovery Review

- a. Ensure all incident reports, investigations and corrective actions have been communicated to affected stakeholders
- b. Determine and agree any remediation steps require

Threat Principles and Procedures

31: Threat Principles and Procedures

This document aims to outline the principles and practises the My Workplace Health team has put in place in order to **prevent** data exposure and unapproved third-party access into the software, as well as assist in adequate responses in the event that a leak is detected.

In order, the document will discuss the *immediate threat notifications* received by My Workplace Health when an intrusion attempt is made, an example of and the results from one of our perimeter scans that occur on a quarterly basis, discuss the standard and major incident response procedures, as well as our compliance with the Notifiable Data Breaches Scheme, and our relevant process flow.

32: Threat Notifications

My Workplace Health is a subscriber of **Imperva**- a cyber security software and services company which provides protection to enterprise data and application software. As a part of this service, My Workplace Health receives immediate email notification at any time when an unauthorised third-party poses a threat on our system.

Examples of threats Imperva reports on includes:

- Illegal Resource Access
- Cross Site Scripting
- SQL Injection
- Bad Bots
- Use of Hacking Tools

In addition to the immediate email alerts, My Workplace Health also receives a weekly summary regarding the threats and attempted intrusion of our system, and how the software adequately responded to this.

An example of the *email notification (1.1)* and the *weekly report (1.2)* are shown below

32.1: Threat Notification Images

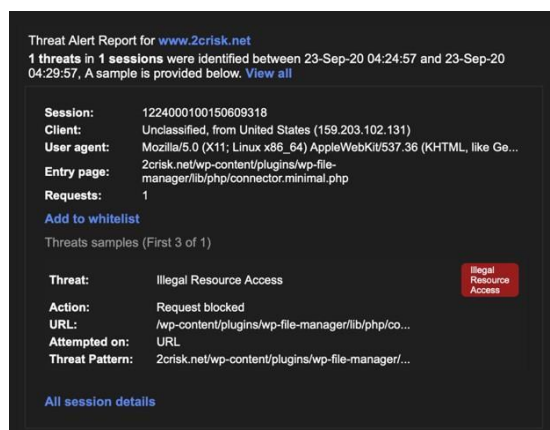


Image 1.1



Weekly Report for Health Risk Management Systems Pty Ltd

Sep 14, 2020 - Sep 21, 2020

Account statistics

Top visiting countries

Australia	98.39%
United States	1.02%
South Africa	0.18%
New Zealand	0.17%
Philippines	0.05%
France	0.04%

Request handling

Returned from cache	0.0%
Passed to origin	99.97%
Blocked	0.03%

Security alerts

Visitors from blacklisted IPs	0
Visitors from blacklisted Countries	59
Visitors from blacklisted URLs	0
Bot Access Control	23
Suspected bots that triggered a CAPTCHA	0

Top attacking countries

United States	14.81%
Ukraine	11.11%
Germany	11.11%
France	11.11%
Russian Federation	7.41%
Poland	7.41%

Cache distribution

Static content	0.0%
Dynamic content	0.0%
Rule based	0.0%

WAF alerts

Remote File Inclusion	0
SQL Injection	0
Cross Site Scripting	1
Illegal Resource Access	3
DDoS	0
Backdoor Protect	0

Image 1.2

33: Perimeter Scans

My Workplace Health runs **perimeter scans** of the software on a quarterly basis. A perimeter scan is defined as “an automated tools that allow organizations to check if their networks, systems and applications have security weaknesses that could expose them to attacks”

My Workplace Health runs these scans in order to prevent future exposure and leaks, as well as use it as a point of discussion for potential improvement or upgrades to our security set up.

An example report from our perimeter scan is attached, **[please view MWH Perimeter Scan 09072020.docx](#)**

34: NDB

The Notifiable Data Breaches Scheme (NDB) under Part III C of the Privacy Act 1988 establishes requirements for entities in responding to data breaches.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 establishes the NDB scheme in Australia from the 22nd February 2018.

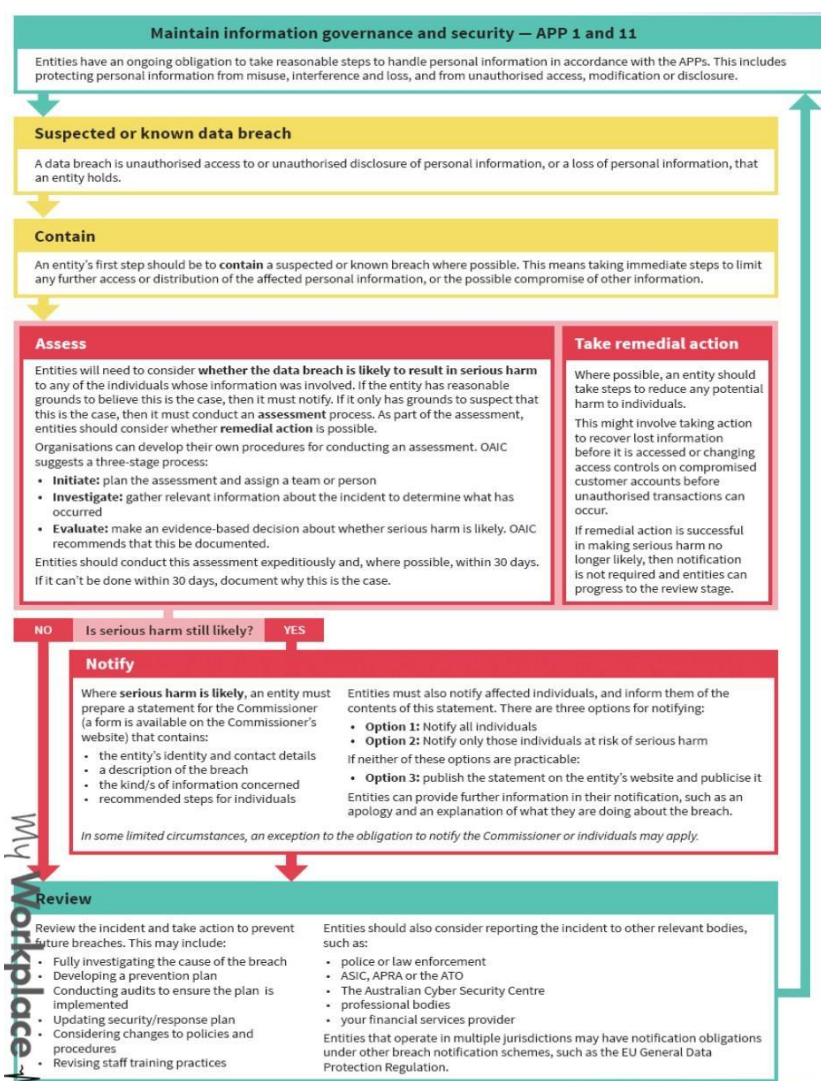
My Workplace Health maintains an eligible data breach statement and includes:

- Identity and contact details of the entity (s26WK(3)(a))
- Description of the eligible data breach (s26WK(3)(b))
- Kind of information involved (s26WK(3)(c))
- Recommended steps (s26WK(3)(d))

All of the above *Daily Threat Notification, Weekly Report and Perimeter Scans* fall in line with My Workplace Health’s compliance with the NDB.

34.1 : Process Flow

On the right is a Process Flow of the steps taken by My Workplace Health in the event of a data breach.



34.2 : NDB Responsibilities

Below outlines the responsibilities of staff and third parties related to My Workplace Health's security response in the event of a data breach.

Name	Responsibility
Mark Cassidy	Chief Executive Officer - Privacy/NDB Manager Direct Contact: 0418 893 291, markc@2CRisk.com.au PO BOX 826, Templestowe, VIC, 3105.
Adam Heppenstall	Chief Technical Officer – My Workplace Health
Mark Prominitz	ItoC Managed Services – Principal Architect
Alex Ninnis	Principal, M&K Lawyers - Legal Representative
Organisation	Details
CFC Underwriting	Underwriters for HRMS (2CRisk) Cyber Insurance 85 Gracechurch Street, London, EC3V 0AA, UK
Lloyds of London	Policy No: ESG00502679 1 Lime Street, London, EC3M 7HA, UK
Policy: ESG00502679 Start: 00.01 LST 05/02/2018	Health Risk Management Systems Pty Ltd SAAS/ASP Software development, installation and maintenance – Organisational Health and Safety Software.

Resources shown in 4.1 and 4.2 can also be found in [**MWH Security Overview v11.pdf**](#)

35: ItoC Incident Response & Reports

ItoC is a *cloud-services specialist organisation* which provides My Workplace Health support and assistance with their cloud-based AWS server.

On top of our own incident and threat response, ItoC also provide a breakdown of the steps they take in both a *major* and *standard* incident occurrence.

To see these breakdowns, please view [**ITOC Major Incident Response.pdf**](#) and [**ITOC Standard Incident Response.pdf**](#) respectively.

Similarly, My Workplace Health and ItoC meet on a monthly basis to discuss and evaluate the uptime and successes of the last 30 days, as well as what can be improved. With this meeting, we are able to ensure that we are optimising our application and get a more in-depth insight into the occurrence of any down-time or incidents.

To see this report, please view [**MWH ItoC Monthly Report.pdf**](#)

Systems Security Model

36: Database Security Model

36.1: Separate Database for each Customer

- A. Each database could be hosted on a single physical server or as multiple virtual servers on a single physical server
- B. Easy to maintain a single database source copy, but increased overhead in implementing changes multiple times
- C. Physically secure but expensive to host and maintain the applications

36.2: Separate Schema for each Customer within single database

- A. Each company's set of tables would be stored in a separate schema and workspace
- B. the overhead of this is separate database scripts created for each implementation
- C. Schema RISK01, RISK02, RISK03 etc
- D. Versions could possible diverge, strong implementation control is needed to maintain each implementation as an exact copy (increased overhead)
- E. Logically secure with in the database, customers could not get at each other's data because of the inbuilt database solution

36.3: 2CRisk Multi-Tenanted Database

- A. 2cRisk is a single database, single schema, and single set of tables
- B. Since all users have potential access to all data, securing the data is enforced by table constraints and programmatically
- C. Logically secured by using database table constraints which means that the application maintainable as an agile methodology.
- D. The user access is controlled through their profile which contains a mandatory database constrained link to a single employer (unique_id), this is controlled at logon via a custom security interface
- E. All records are foreign keyed to the employer and can only be created, modified and retrieved using the employers unique key.

37: Integrated Development Environment

37.1: IDE: Oracle Application Express

1. This IDE is a web-based tool that stores the application in the Oracle Database
2. APEX is a rapid application development (RAD) tool which renders the web pages as HTML5 at execution time
3. Users only require a standard browser to access the system there is no client deployment of any kind.
4. Apex enforces web2 standards by using cascading style sheets, html5, ajax and JavaScript.
5. Advantages of APEX are performance, the fastest way to access an Oracle data is PL/SQL the language used by Apex
6. The Apex IDE has built in Oracle security to control access for developers and end users if required.

37.2: Administration System

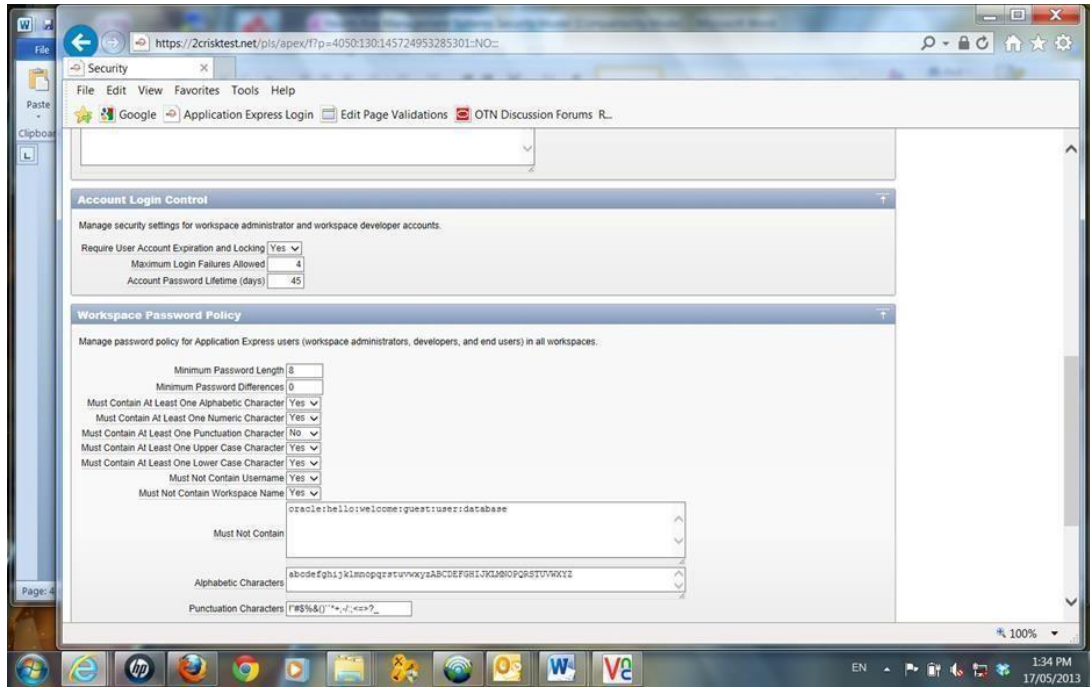
- A. Manage Requests
- B. Runs in manual provisioning mode
- C. Manage Instance
 1. Instance Settings
 - a) Feature configuration
 - b) Security
 - c) Instance settings
 - d) Workspace purge settings
 - e) Manage new service signup wizard
- D. Manage Meta Data
 1. Session state
 2. Mail Queue
 3. Installed Translations
- E. Manage Shared Components
 1. Public Themes
 2. Template Applications
- F. Messages
 1. Define login message
 2. Define system message
 3. Manage site-specific tasks
- G. Manage Logs and Files
 1. SQL workshop logs
 2. Page view activity logs
 3. Developer activity logs
 4. External click counting log
 5. Login access log

37.3: Manage Workspaces

- A. Workspace actions
- B. Workspace reports
- C. Export Import
- D. Manage Applications

37.4 : Monitor Activity & IDE Administration Password Rules

1. Page views
2. Service requests
3. Workspace purge
4. Logs
5. IDE Administration Password Rules



The Apex Administration system configures the Session Timeout parameters
Maximum Session Length in Seconds => 28800
Maximum Session Idle Seconds => 1800

38: APEX Protection against External Security Threats

Apex is written to prevent the following Web Security Threats:

38.1 : SQL Injection

- a. SQL injection is a security breach that augments the SQL in the application with addition SQL language constructs, often using an input field that might be concatenated into a SQL predicate.
- b. Prevented by using bind parameters

38.2 : Cross-Site Scripting

- a. Cross-site scripting (also referred to as XSS) is a security breach that takes advantage of dynamically generated Web pages
- b. In an XSS attack, a Web application is sent a script that activates when it is read by a user's browser
- c. Once activated such a script can steal, data, including session credentials, and route the information to the attacker.
- d. To prevent this from happening, special characters should be escaped.

38.3 : URL Tampering

- a. URL tampering refers to any practice where the URL is modified within the navigation panel in order to gain access to pages, privileges or information that is not available using ordinary navigation options within the application
- b. To prevent this from happening, Apex provides Session State Protection.

38.4 : Eavesdropping

- a. The best defence against eavesdropping of any kind is to establish a secure connection between the web browser and the Apex application server.
- b. Imposing SSL on a HTTP connection makes it an HTTPS connection
- c. Apex brokering schemes support HTTPS and Apex can even be configured to *require* that all of its connections be secure connections.

39: My Workplace Health Applications & Security

MWH consists of 3 separate applications:

39.1: Company Administration

- a. Creates and maintains Individual Companies and their associated global configuration
- b. Set companies module access
- c. Create company administration users
- d. Job Scheduler
- e. Application Online Documentation
- f. Maintain Password Rules
- g. Maintains all system wide reference data
- h. Session Timeout
 - i. Maximum Session Length in Seconds => 28800
 - ii. Maximum Session Idle Seconds => 3600

39.2: Client Administration

- a. Set Company Globules (password expiry)
- b. Set Company reference data (sites, occupations)
- c. Data Integration
- d. Company Application Defaults limits (questionnaires, threat hold limits)
- e. User authentication (reset password)
- f. User authorisation
- g. All application data changes are audited
- h. Session Timeout
 - i. Maximum Session Length in Seconds
 - i. Maximum Session Length in Seconds => 28800
 - ii. Maximum Session Idle Seconds => 3600

39.3: Health Risk Management

- a. Employment Medicals
- b. Health Management
- c. Injury Management
- d. Injury Cost Management
- e. Exit Medical
- f. Health Intelligence
- g. All application data changes are audited
- h. Session Timeout
 - i. Maximum Session Length in Seconds
 - a. Maximum Session Length in Seconds => 28800
 - b. Maximum Session Idle Seconds => 3600

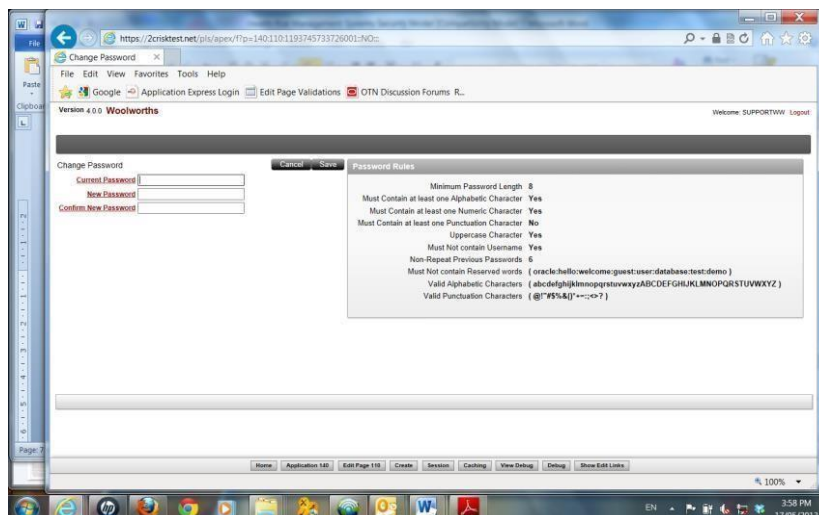
39.4: Application Security Framework

- a. 2CRisk Company Administration: Username are defined and administered in Apex IDE Administration; the list is Health Risk Management Systems internal personnel only.

39.5: 2CRisk Client Administration and 2cRisk Health Risk Management

- a. User's 2CRisk custom security module that encrypts the password entered, and then compares that encrypted value against the stored encrypted password for that username.
- b. Password encryption uses one way encryption that cannot be decrypted.
- c. Once a password is Reset by a Company Administrator the user must then change the password again the first time they attempt to logon.

- d. The maximum number of failed logons is Defaulted (3) but can be changed on an individual company basis
- e. The only way to unlock a username with 3 failed logons is for an administrator to Reset the password.
- f. In client administration there are permission settings to allow authorisation for the creation, updating and reading of data by user by module.



40: Database Passwords Procedure

All Oracle 12c database passwords are controlled and set by Health Risk Management Systems personnel all passwords obey strong password rules as defined by Oracle. The same password rules as being imposed as the 2cRisk password rules. This section applies to the organisation's servers.

41: UNIX Red Hat OS & Virtual Private Network Passwords

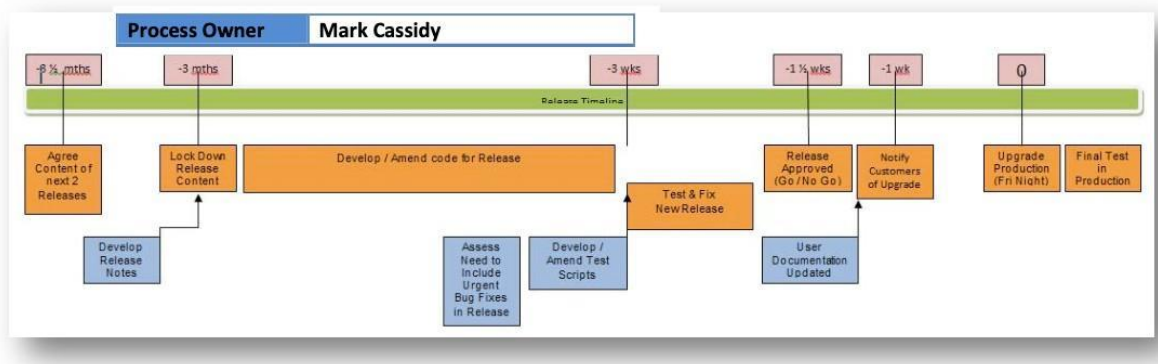
ITOC control the setting of OS and VPN passwords which also obey strong password rules. ITOC supply all our OS patching, SSL Certificates and VPN support.

Version, Releases and Change

42: Release Management in the SaaS Model

The standard 2CRisk release process is detailed in the chart below. Effectively 2CRisk maintains one Production environment (multi tenanted), one Test Environment and one Development Environment (internal only) across all clients.

Once a change management request has been received and approved, a version-controlled Enhancement Document (sample attached) is produced and agreed upon.



42.1 : An Individual's Input on RM

- Once a change request has been identified, it is communicated to 2CRisk using normal procedures involving the Client Manager.
- Agreement is made on the scope of the requirements.
- A 2CRisk design document is produced and released to the client for consideration and approval.
- Once the design document has been approved, a Change Request (CR) document is produced which includes:
 - Area Affected (i.e. Employment Medical, Self-Service app etc)
 - Business Priority
 - Current Situation
 - Description of change
 - Impact Analysis (what impacts the changes will have on the system)
 - Costing, Resourcing, Timing and other considerations.
- Once the CR has been approved, a decision, in consultation with the client, is made, whether this is an urgent upgrade or change, or whether it can go into our normal release process as detailed previously. An example of this would be inclusion of classification changes, whereby they may not be urgent but are require for reporting purposes and can be included and bundled with upcoming, planned system releases.
- An internal assessment (Impact Analysis above) is carried out to ascertain whether the changes are going to impact on other customers and or whether they can be incorporated across the platform in such a way that it does not impact on other customers. An example of this would be the inclusion of the 2 Factor Authentication requirements. This has been built into the system allowing it to be "Switched on" for clients as needed and as such, does not impact on existing clients.

42.2: Prioritisation of Change

Once again, this is mainly done in consultation with the client and it does involve an internal assessment over whether the changes will impact on the overall system architecture or just on an individual client's partitioned access to 2CRisk.

Our system perspective is to ensure that our solution in the marketplace meets and exceeds our customer requirements and that, where possible, any changes that are made to the solution architecture are an overall enhancement of the software.

In some instances, 2CRisk endeavours to engage with our customer base to build consensus across the solution requirements. An example of this is with the Injury Management application where the overall functionality of this application is essentially the same for every client (meeting regulatory needs etc), but enhancements can be developed that have a "suitability and fit" for all customers.

In terms of deciding on what priorities for development and release are undertaken and indeed when, our focus is generally speaking aimed at meeting individual customer needs whenever possible.

42.3: Release Process

Please refer to the process diagram provided in this document. Generally speaking, we do involve clients in testing for new releases. Some clients do not feel they need to get this involved whilst others are very keen to be involved in testing.

Conceptually 2CRisk carry out testing of new developments in our Testing Environment, with direct client involvement in the Test Environment. Once testing has been completed, clients are run through the changes prior to developments being moved over into the Production Environment. This forms a part of our UAT (User Acceptance Testing) and PVT (Post Verification Testing).

An example of this would be with development of the Event Management Application with Ambulance Victoria. As this application centred on primarily psychological wellbeing for emergency services and similar organisations, it stands to reason that we would develop this in partnership with a customer.

The process followed using this example was that 2CRisk carried out the conceptual work with the client using mock up's and screen shots to get consensus. Once this was done, we produced the changes in our development environment and then into the Test Environment for thorough testing.

Generally speaking, this client was involved and formal acceptance prior to the changes being moved into the Production Environment, where UAT was undertaken.

42.4: Communication Points

Please refer to the process diagram provided in this document.

42.5: Expectation of Communication Materials

Whenever there are outages in the system, for example, when new upgrades, enhancements or maintenance carried out, a support email is sent to all customer and partners to advise of the outage and reasons thereof. An example is provided below.



42.6: Implementation Assessment Criteria

1. Assess the need
2. Produce a design document
3. Produce a CR document for approval
4. Develop/Amend code for release
5. Develop/Amend test scripts (UAT/PVT)
6. Carry out testing in Development environment
7. Once ready, move from development environment to test environment
8. Complete testing in Test Environments.
9. Feedback with clients as needed.
10. Sign off
11. Lock down release content
12. Develop release notes/training material
13. Test/Fix new release

43: Release Management FAQ

If another client's change is bundled with our changes for a weekend, and the other clients change fails PVT, what happens to the release – fix on fail or rollback? What if our change is urgent and passes?

Using this scenario, we would continue with the client CR and implement as a standalone.

Generally speaking, the normal approach is that items are not bundled into release until they have been thoroughly tested in both the Development site and the Test site.

2CRisk maintains a Quick Release Strategy

- Only Driven by urgent customer need or urgent bug fixes
- Must be approved by Mark Cassidy MD and Adam Heppenstall CTO
- Basic Process Steps to be followed
- Development Timescale Will Be Reduced
- Testing & Notification Timeline remains constant

Will each release have a rollback plan documented and tested prior to deployment?

The rollback plan for each release is that if something goes wrong after migrating the latest release from test to production, we can reverse the migration and return the system to the point prior to the migration.

If another client proposes to change to functionality which we are also using, how can we choose to be involved in UAT or not?

Yes. If there are material changes to the underlying structure of the software (as opposed to functionality that can be adjusted to meet specific needs), we would communicate any proposed changes to existing customers for feedback and involvement if required. Generally speaking, if we feel that the changes are for the betterment of the software for all users, we may choose to partner in a financial sense to bring the release to fruition and thus making it available to all customers as a value add.

What changes affect all clients, vs an individual?

Changes to the underlying platform of 2CRisk affect all clients as we maintain only one Production Environment of 2CRisk. Each client portal has the ability to create and modify aspects of the software, specifically in the Administration application such as reference data, building medicals, JTA's, risk scoring, building health services and creating users and security roles etc.

See Images Below

Changes can be made to the underlying platform that does not impact on other customers. For example, the recent 2 Factor Authentication security has been created and adopted at a system architecture level but has not been switched on for other customer to use at this point in time.

See Images Below

If we raise a CR – can we please get a cost/timeline back before build commences so we can assess whether to go forward with the change? Is there a certain CR form you want us to fill in?

Yes

Can we start getting Design Documentation back after we raise a CR, before build commences

Most certainly and this is our preferred way of operation. Under normal operating circumstances, our preferred way would be to develop a CR, including costings prior to any design document being agreed upon.

How does the emergency fix process work?

Emergency fixes can be introduced at either a system level or a client level depending upon the overall impact on the system architecture.

If the emergency/bug fix is required to address an immediate issue, this is usually done on the same business day, after hours, with clients overseas who may be affected, notified by the relevant Client Manager via email/telephone with a view of minimising any disruption where possible.

44: Release Management Images

Function	Step	Action	Issue No	Issues	Suggested Correction	Priority	Status	Comments
			53					
			54					
			59					
			70					
			71					
			72					
			73					

UAT/PVT Testing Spreadsheet

PROCEDURE: QUALITY ASSESSMENT PROCESS TESTING
PROCEDURE No: 2CR002

2CRisk™

CLIENT MEDICAL TESTING DOCUMENT

Client	XXXXXXXXXX	Owner	Mark Cassidy
Scenario	How do I create an applicant manually?	Status	In test
Description	Test capacity for user to manage manual creation	Test Release Date:	DD/MM/YYYY
Expected Results	Software performs as expected	Expected completion	DD/MM/YYYY

SCENARIO TO BE TESTED

How do I create an applicant manually?

DESCRIPTION

As a system user with access to the Employment Medical application, users need to be able to go into the system and manually create an applicant for a pre-employment medical. Whilst the XXXXX normal process will involve loading candidates via the csv file function (Administration User), from time to time, users may be required to manually load an applicant into the system.

This test involves a system user with log in and access credentials to the Employment Medical application being able to:

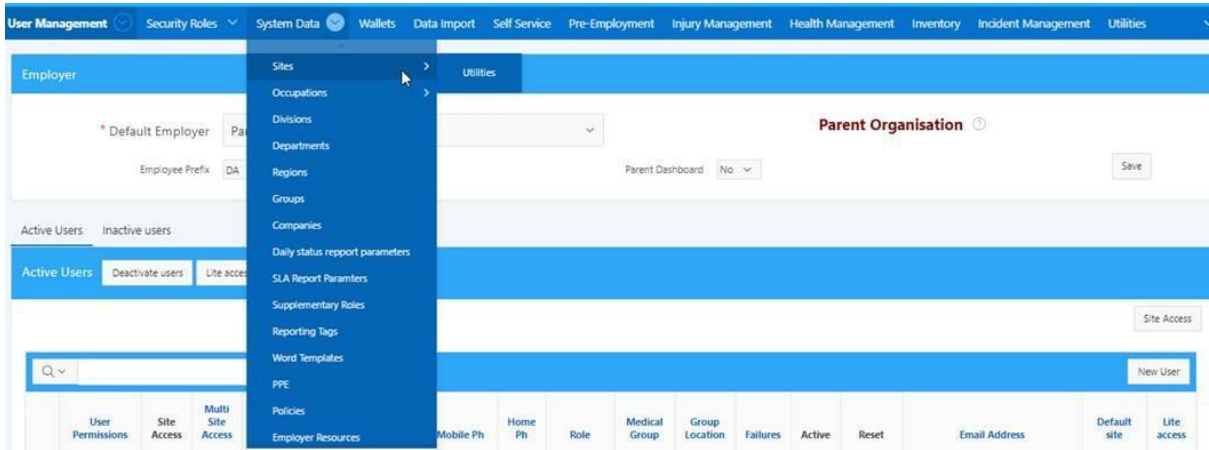
- Enter into the Employment Application
- Search for the applicant if required including archive searching
- Create an applicant and enter relevant fields of information
- Attach an occupation and a site for the applicant
- Create the Applicant

Example UAT/PVT Testing Document

EMPLOYMENT MEDICAL			
What was tested	Function	Your comments	Pass/Fail
Create an applicant (manually) in the Employment Medical application	Create Applicant		
As a user with access to Employment Medical	Log in screen		
<ul style="list-style-type: none"> Logs into the System Clicks on Employment Medical Opens to Applications Page Clicks on the radio button for archive Enter the surname of the new candidate (surname Healthy) Clicks on GO Row Test should return – "no data found" Click on the "x" to cancel the search User should return to the Applications Page User clicks on "New Application" User clicks on "New Applicant" 	User access User access Employment Applications Archive Radio Button Search Function Search Function Search Function Search Function Employment Applications New Application function New Applicant Function		
User will now create a new Applicant but in doing so, testing must involve the intentional missing of required data fields	Create new Applicant		
<ul style="list-style-type: none"> User enters last name only (Last Name: Healthy) User clicks on create 	Create applicant Create function		
An error report should appear at the top of the screen, in yellow, advising	Error reporting		

UAT Content Sheet

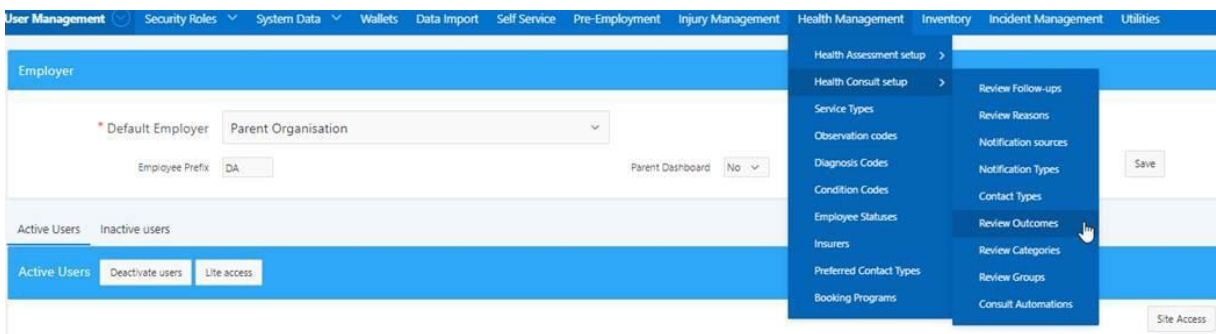
Two-Factor Authentication



Adding Email Template, Privacy Policy and Healthy Me Users



Adding pre-employment reference data, medicals, etc.



Adding Health Management Reference Data

Active Users Inactive users

Active Users Deactivate users Lite access

Site Access

Q Go Actions New User

	User Permissions	Site Access	Multi Site Access	Employer Child Access	Work Ph	Position	Mobile Ph	Home Ph	Role	Medical Group	Group Location	Failures	Active	Reset	Email Address	Default site	Lite access
	cassioymark					External Provider	0433444551		PROVIDER			0	Y	Password	markc@2crisk.com.au		Y
	cdilivereport								Child Live Reporting			0	Y	Password	richard@2crisk.com.au		N

Adding active and inactive users with security roles, site access and authentication provisions