METROPOLIS HEALTHCARE INFORMATION SECURITY ORGANISATION POLICY

Approval date:	
Review date:	
Author:	Mulla Ibrahim – Information Security
Approver	Abdur Razzaque - Group IT Head
Classification	Internal
Document number:	GL-MHL/POLICY/IT/10/V-I
Version number:	Draft

Table of Contents

1 Introduction

Metropolis is a strong and highly trusted pathology specialist in the Indian diagnostic space and conduct millions of test every year globally and each of the test are focussed to deliver precision and accuracy

MHL's systems and services form part of a complex ecosystem, which work cohesively to provide critical Healthcare services. To deliver these services, MHL utilise a mixture of Information Technology (IT) and Operational Technology (OT).

It is important that the use of information, systems and services are controlled to protect against computer misuse, reduce unnecessary risk to the company and to ensure that MHL continues to meet the legal and compliance obligations.

2 Purpose

2.1 The purpose of this policy is to set out MHL's strategic direction on and commitment to Information Security. It defines the context of Information Security within MHL, the related responsibilities and the information security principles that should be followed by all colleagues and third parties working for or on behalf of MHL.

2.2 Within MHL, information security also encompasses the term "Cyber security" and all organisational activity associated with cyber, therefore the terms be interchangeable in this context.

3 Scope

3.1 This policy applies to:

- All information, systems and services developed, owned and operated by MHL or on its behalf.

3.2 This Policy also applies to the following.

- MHL colleagues
- Contingent Workers
- Third Party Suppliers

3.3 This policy must be complied to with when working or using any corporate or personal device, whether on-site or remotely that is connecting to or using any MHL information, systems and services.

4 Information Security at Metropolis Healthcare

Information security is concerned with ensuring the Confidentiality, Integrity and Availability of information, systems and services. MHL is committed to satisfying legal and compliance requirements in relation to information security including but not limited to compliance Draft India Personal Data Protection Bill (PDPB)-2019

MHL has dedicated people, processes and technology that work together in order to mitigate identified risks and help protect systems and information.

MHL has implemented an Information Security Management System (ISMS), which provides the framework that governs security management activity and supports the protection of critical systems, information and services provided across the organisation. MHL is committed to continually improving the ISMS and associated information security controls implemented.

5 Policy Statements

5.1 Information, systems and services shall be protected against unauthorised access, loss and corruption through the application of relevant, proportionate and up to date security approaches and controls, which have been defined through a risk assessment.

5.2 Information, systems and services shall only be made available to authorised individuals with appropriate business justification and in accordance with the MHL Identity and Access Management Policy.

5.3 Information, systems and services shall be classified, handled and disposed of, in accordance with the requirements of the MHL Information Classification and Handling Standard.

5.4 Authorised individuals with appropriate business justification using MHL information, systems and services shall follow and comply with the MHL Acceptable Usage Policy and any other specific requirements as determined by MHL.

5.5 Authorised individuals with appropriate business justification who are provided with access to MHL's information and information systems, shall have regular and appropriate information security awareness, training and guidance.

5.6 Systems and services shall be risk assessed at planned intervals, when significant changes occur or upon change in threat. Any risks identified shall be recorded in a risk register and be mitigated. Identified risks shall also have assigned owners who are responsible for understanding and making decisions on risk.

5.7 Information security policies, standards, procedures, processes and controls shall be formally documented and must be followed.

5.8 Information security policies, standards, procedures, processes and controls shall be regularly reviewed to verify they are being adhered to.

5.9 Information systems shall be reviewed at planned intervals, when significant changes occur or upon change in threat to ensure compliance with MHL's policies, standards and procedures.

5.10 Information security shall be independently assessed and tested at planned intervals and when significant changes occur, to ensure security controls are operating effectively.

5.11 Information systems shall be continuously monitored to identify unauthorised access, computer misuse, loss, malfunction or corruption.

5.12 MHL has clearly defined objectives established that drive the ISMS. Objectives shall be time-bound and monitored for effectiveness. Where appropriate, projects and programmes shall also include information security objectives, and these shall also be timebound.

5.13 All third parties processing MHL information or operating MHL systems and services must comply with the policy on Information Security Requirements for Third Parties. This includes but is not limited to, responding to information security assessments, identifying risks to MHL and supporting risk remediation activity.

5.14 If any user of MHL information or information systems becomes aware of any actual or potential loss or incidents, anomalies, misuse or vulnerability of such information or Information Systems, then they must report it immediately to the IT Service Desk.

6 Accountabilities and Responsibilities

6.1 This policy is managed by the Information Security Team and approved by the Board of Directors.

7 Consequences of the Policy

7.1 Where it is suspected that this policy is not being followed by MHL employees, the matter may be dealt with in accordance with the provisions of the Disciplinary Policy as amended from time to time.

7.2 Where it is suspected that this policy is not being followed by contingent workers or third party suppliers the matter will be dealt with in accordance with the provisions of the Disciplinary Policy and/or on via a contractual basis where the contingent workers and/or third party supplier is bound by contract.

8 Exceptions to this policy

8.1 In general, there shall be no exceptions granted to this policy. However, if there are situations where compliance is deemed not achievable, then the Information Security team shall be consulted for further guidance.

9 Communication of the policy

9.1 This policy can be found on the Teams SharePoint. Managers and sponsors of third party suppliers shall communicate this policy to all MHL employees, contingent workers and third party suppliers.

10 Management review of the Policy

10.1 This policy will be reviewed on an annual basis or whenever a change is required.

11 Appendices

Appendix A – Definitions

These definitions apply to the Information Security Policy:

Business Purpose a legitimate reason to conduct an activity that is directly related with the services provided by MHL.

Contingent Worker: a contracted individual that is undertaking a permanent or temporary role in the capacity of a permanent employee but is supplied and paid by a Third-Party Supplier.

MHL Employee: Someone who holds a direct employment contract with MHL and is paid directly by MHL on permanent, temporary or fixed term contracts.

Information: all data owned by MHL or processed on its behalf that can be structured to acquire meaning, relevance and purpose in whatever form, including but not limited to documents, emails and webpages.

Information Security: protecting the confidentiality, integrity and availability properties of MHL Information and Information Systems.

Information Systems: (i) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (ii) digital data stored, processed, retrieved or transmitted for the purposes of their operation, use, protection and maintenance, including networks and domains.

Third Party Supplier: a third-party organisation or an individual employed by a third-party organisation that has contracted with MHL to provide services to MHL