IT Security Policy

Introduction 2
Scope of Policy 2
Purpose of Policy 2
Definitions 2
Responsibilities 3
Information Security Management Systems (ISMS) 4
Risk Management 4
Equipment Security 4
Access Controls 5
Access to Secure Areas 5
User Access Control 5
Security Incident Management 5
Housekeeping 6
Data Validation 7
Software Protection 7
Data Network Security 8
Disaster/Recovery Planning 8
Email and Internet 9
Dissemination of Document 9
References 9

Introduction

In order to provide education, training, assessment, qualifications and health and safety measures to its customers and clients, the Mineral Products Qualifications Council (MPQC) needs to gather, process, store and use certain information which is stored on its IT Systems. Data stored in information systems represents an increasingly valuable asset to MPQC as systems proliferate and increased reliance is placed on them.

MPQC seeks to protect its information systems from misuse and to minimise the impact of service breaks by developing this Information Security Policy and procedures to manage and enforce it.

Scope of Policy

This policy covers IT Security for all databases and systems which includes, but is not restricted to:

- Nexus and mp connect
- Physical IT Servers and other IT infrastructure (e.g., laptops)
- Cloud Servers

Purpose of the Policy

The purpose of the policy is to ensure that:

- Security: MPQC's IT information systems are properly assessed for security.
- Confidentiality: Data access is confined to those with specified authority to view the data.
- Integrity: All system assets are operating correctly according to specification and in the way the current user believes them to be operating.
- Availability: Information is delivered to the right person when it is needed.
- Responsibility: Staff are aware of their responsibilities, roles, and accountability; and
- Breaches: Procedures to detect and resolve security breaches are in place

Definitions

Asset - Anything that has value to MPQC, its business operations and its continuity.

Availability - The property of being accessible and usable upon demand by an authorised entity.

Confidentiality - The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

DPO – The Data Protection Officer for MPQC.

Information Security - The preservation of confidentiality, integrity, and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved

Information Security Management System (ISMS) - That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

Integrity - The property of safeguarding the accuracy and completeness of assets.

Mitigation - Limitation of the negative consequence of a particular event.

Risk - The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to MPQC.

Risk Assessment - The overall process of risk analysis and risk evaluation.

Risk Management - The process of coordinating activities to direct and control an organisation regarding risk.

Third Party – The third party in this agreement refers to Octavian IT Limited who are contracted to maintain all MPQC's IT security.

Responsibilities

- Allocating responsibilities for the management of Information Security; and
- Ensuring that, where appropriate, staff receive information security awareness information

Data Protection Officer
The DPO is responsible for the implementation and enforcement of the Information Security Policy, and has responsibility for:

- Monitoring and reporting on the state of information security for MPQC
- Ensuring that the Information Security Policy is implemented throughout the company
- Developing and enforcing detailed procedures to maintain security
- Ensuring compliance with relevant legislation
- Ensuring that personnel are aware of their responsibilities and accountability for information security
- Acting as point of contact on information security for both staff and external organisations
- Implementing an effective framework for the management of security
- Advising on the content and implementation of the information security programme
- Co-ordinating the production of organisational standards, procedures, and guidance on information security matters
- The development and implementation of the Information Security Management System to work towards compliance with the requirements of BS ISO/IEC 27001

General Managers and Managers
MPQC Management are directly responsible for:

- Ensuring that all current and future staff are instructed in their security responsibilities
- Ensuring that all their staff using information systems are trained in their use
- Determining which individuals are to be given authority to access specific information systems. The level of access to specific systems should be on a job function need, independent of status
- Implementing procedures to minimise exposure to fraud/theft/disruption of its systems
- Ensuring that current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability
- Ensuring that all staff read and understand the relevant IT Security clause contained within the staff handbook as part of their contract of employment
- Ensuring that the relevant systems managers are advised immediately about staff changes affecting computer access (e.g., job function changes/leaving department or organisation) so that passwords may be withdrawn/deleted
- Ensuring that any actual or potential breach of information security policy within their area of responsibility is reported to the Data Protection Officer

Staff
All employees and anyone working on behalf of MPQC, involved in the receipt, handling, or communication of information, must adhere to this policy to support the reputation of MPQC.
Each employee will be personally responsible for ensuring that no breaches of hardware or software security result from their actions.

Information Security Management System (ISMS)

MPQC is fully committed to the goals and principles of information security and to manage information security effectively an Information Security Management System (ISMS) will be developed to provide a framework for information security.
Effective information security involves more than simply installing a security product, implementing anti-malware software, providing a security policy, or signing a contract with a support service provider. The ISMS provides a means to identify and co-ordinate the approach to the management of information security by MPQC in order to protect it and its business partners.

The process to be adopted by MPQC reflects the requirements of ISO 27001 by emphasising the importance of:

- Understanding MPQC's information security requirements and the need to establish policy and objectives for information security;
- Implementing and operating controls to manage information security risks in the context of MPQC's overall business risks;
- Monitoring and reviewing the performance and effectiveness of the ISMS; and
- Continual improvement based on objective measurement

Risk Management

MPQC will identify and counter possible threats to the security policy and standards.
All systems will be subject to periodic security reviews by the Data Protection Officer and Octavian. These include both regular quarterly reviews and ad hoc reviews as part of the overall MPQC Risk Register review. Individual systems should be periodically reviewed.

Reviews will include:

- Identification of assets of the system
- Evaluation of potential risks/threats
- Assessment of likelihood of threats occurring
- Identification of practical cost-effective counter measures
- Implementation programme for counter measures (contingency plans)

Systems are liable to independent reviews by internal and external auditors.

Equipment Security

To protect MPQC's equipment against loss or damage and avoid interruption to business activity.
IT equipment will always be installed and sited in accordance with the manufacturer's specification.
Environmental controls will be installed to protect central/key equipment. Such controls will trigger alarms if environmental problems occur. In such cases only authorised entry will be permitted.
Smoking, drinking, and eating is not allowed in areas housing central/key computer equipment and doors should be kept locked.

Equipment Maintenance

All central processing equipment, including file servers, will be covered by third party maintenance agreements.
All personal computers, terminals and printers will be covered by maintenance agreements with the same third party for repair of out of warranty equipment provided it is cost effective (each case will be judged on its merits). All such repairs will only be made on approval by the General Manager for shared services.
All such third parties will be required to sign confidentially agreements.
Records of all faults/suspected faults will be recorded and maintained on the third-party IT helpdesk system.

Remote Diagnostic Services

A third party have been granted remote access to such systems on request to investigate/fix faults.

The connection will be made through an authenticated Remote Access Server. All activity will be monitored.

Security of Hard Disks
Hard disks on any machine may contain sensitive/confidential data. Removal off site of faulty disks represents a potential threat to MPQC. Each such case will only be given to the approved third-party repairers who will have signed confidentiality agreements. Whenever possible the data and information should be overwritten, or the equipment degaussed. Obsolete or faulty Hard Drives will be disposed of in a confidential manner.

Disposal of Equipment
Computer hardware disposal can only be authorised by the General Manager of Shared Services granted to the third party. They will ensure that data storage devices are purged of sensitive data before disposal or securely destroyed in accordance with their disposal procedures.
Unusable computer media should be destroyed in accordance with the same procedure.

Access Controls
To identify the location of MPQC's systems assets this includes:

Physical Assets
An up-to-date register of acquisitions and disposals of physical computer assets will be maintained, this will include the Department, name of staff member and serial number. A Shared Services member of staff will maintain this asset register.

Software
It is the responsibility of the General Manager for Shared Services and the third party to hold licenses for all software loaded on MPQC's computer systems. Any software procurement will only take place after approval of the General Manager for Shared Services.

Access Control to Secure Areas
To minimise the threat to MPQC's information systems through damage or interference.

Physical Security
MPQC's central processors/networked file servers/central network equipment is located in secure areas with restricted access.

Entry Controls
Access to the central computer facilities will be confined to designated staff, whose job function requires access to that particular area/equipment. Restricted access to other staff, where there is a specific job function need for such access, will be granted by the General Manager Shared Services on a temporary basis.

User Access Control
To control individual's access to systems and drives that are required for their job function.
Access privileges will be modified/removed - as appropriate - when an individual changes job/leaves.

User Password Management
No individual will be given access to a live data system unless properly trained and made aware of their security responsibilities.
Users should keep their passwords secret and never disclose them to colleagues.
Passwords should be changed regularly - all new systems will include password ageing to force users to change their password periodically.

Security Incident Management
To detect, investigate and resolve any suspected/actual information system security breach.

A security incident is an event that may result in one or more of the following:

- Degraded system integrity
- Loss of system availability
- Disclosure of confidential information
- Disruption of activity
- Financial loss
- Legal action
- Unauthorised access to applications.

All instances of incidents involving the mismanagement of information should be reported to the Data Protection Officer for further investigation as appropriate and may need to report to the Information Commissioners Office (ICO). Information Security breaches may result in disciplinary action.

Individual's Responsibilities
Each information user is personally responsible for ensuring that no actual or potential security breaches occur as a result of their actions.
Computer users should ensure that they do not disclose their passwords or allow anyone else to use their password or allow another user to work under their log on.
Passwords that have potentially been compromised should be changed by the user immediately.

Housekeeping

To maintain the integrity and availability of computer assets.

Data Backup
All central systems have formalised backup policies for each category. Backups are checked on a quarterly basis jointly by General Manager Shared Services and the third party. The Nexus server is hosted remotely in Microsoft Azure, with Azure backup provided.
All onsite servers are backed up individually and follow the below schedule and polices:

Incremental backups
Such backups have a minimum of a 6-day cycle before any data is overwritten. Incremental backups are taken and verified every 15 minutes between the hours of 8:30am to 5pm Monday – Friday.
Consolidated Daily backups
The above backups are then consolidated at the end of each day to one file that is retained for 10 days
Consolidated Weekly backups
The above backups are then consolidated at the end of each week, and these are retained for 30 days
Consolidated Monthly Backups
The above backups are consolidated at the end of each month and retained for 6 months. Anything older than this is included in a consolidated roll-up file with no deletion.
Replication
Backups are first taken to another drive within MPQC's main server at MP House and then Consolidated Daily backups are replicated to StorageCraft cloud and retained for 3 working days

Incident Reporting
MPQC's central systems will have formal incident recording and escalation procedures, currently under development.
Incident recording will be used to log all unusual events. This mechanism will include what happened, what was done and final resolution.
Major incident control procedures will be used to manage serious problems e.g., inability to recover critical live systems.

Media Disposal
To ensure data confidentiality all obsolete removable media will be disposed of via the third-party IT provider who will arrange appropriate confidential disposal and destruction.

Data Validation
To maintain confidence in data accuracy for use in decision making.

At Data Input
Data accuracy is the direct responsibility of the person inputting the data supported by their line manager. All systems will include validation processes at data input to check in full or in part the acceptability of the data. Depending on the system, later validation may be necessary to maintain referential integrity. Systems should report all errors together with a helpful reason for the rejection to facilitate correction. Error correction should be done at the source of input as soon as it is detected. Such correction is increasingly important as systems are linked and errors can be transmitted between systems.
Any loss or corruption of data should be reported to the relevant system manager at once.

Internal Validation
All systems will incorporate internal validation processes and audit trails to detect and record problems with processing/data integrity.

Software Protection
To comply with the law on licensed products and minimise risk of computer viruses.

Licensed Software
All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. The third-party IT provider will be responsible for holding copies of all licenses.

Software Standards
MPQC will only permit approved software to be installed on its PCs. Approval will be via the third-party IT provider. MPQC will require the use of specific general-purpose packages (e.g., word- processing, spreadsheets, databases) to facilitate support and staff mobility.
MPQC recognises the need for specific specialised PC products, such products should be approved and registered with the General Manager for Shared Services and be fully licensed.
Shareware programs are only free when under evaluation. Full licences should be purchased if the program is used for MPQC business. Freeware is totally free, but all Users should seek guidance from the third-party IT provider on the correct use of both Shareware and Freeware.
Users should not load any software onto MPQC PCs without the prior approval of the third-party IT provider and General Manager for Shared Services.

Virus Control
MPQC seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software loaded on all Networked PCs and Servers.
Users should report any viruses detected/suspected on their machines immediately to the General Manager for Shared Services and the third-party IT provider.
No newly acquired disks/CDs from whatever source are to be loaded unless they have previously been virus checked by the locally installed virus checking package. USB drives and other portable media must also be scanned for viruses prior to use.
The third-party IT provider are responsible for installing and updating the Anti-Virus software. Virus databases will be updated on a regular basis and all networked systems and users will be protected. All

devices connected to MPQC's network will automatically have anti-virus software loaded.

Data Network Security

To be able to ensure the security of MPQC's Data Network. The third-party IT provider will:

- Ensure availability.
- Ensure that the network is limited to authorised users.
- Preserve the integrity of all data and information on the network.
- Protect the network from unauthorised or accidental modification ensuring the accuracy and completeness of their assets.
- Preserve confidentiality; and
- Protect against unauthorised disclosure

Data Network Definition

The Data Network is a collection of communication equipment such as LAN switches, routers, servers, computers, printers, which have been linked. The network is created to share data, software, and peripherals such as printers, fax machines, internet/email connections, hard disks, and other storage equipment.

Network Security Policy

This policy applies to all networks within MPQC.

To satisfy this MPQC will undertake the following:

- Protect all hardware, software, and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non- technical measures.
- Provide both effective and cost-effective protection commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost-effective manner.
- Compliance with the following:
    - Computer Misuse Act 1990;
    - Data Protection Act 1998;
    - Electronic Communication Act 2000;

Disaster Recovery/ Planning

To be able to restore computer facilities to maintain essential business activities following a major failure or disaster.

Need for Effective Plans

MPQC recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event on its core business through tested disaster recovery plans.

MPQC recognises that IT systems are increasingly critical to its business and that the protracted loss of key systems/user areas could be highly damaging in operational terms.

Planning Process

The main elements of this process will include:

- Identification of critical computer systems.
- Identification and prioritisation of key users/user areas.
- Agreement with users to identify disaster scenarios and what levels of disaster recovery are required.
- Identification of areas of greatest vulnerability based on risk assessment.
- Mitigation of risks by developing resilience; and

- Developing, documenting, and testing disaster recovery plans to identify tasks, agreeing responsibilities, and defining priorities.

Email and Internet

To control and monitor the use of email and the Internet. To protect MPQC and the users from misuse.

User Agreements

Users of MPQC's Email system and connection to the Internet will be given a copy of MPQC's Internet and Email Acceptable Use Policy. New accounts will not be enabled until the user signs and returns the acknowledgement slip to the General Manager for Shared Services.

Protecting Personal Use During Absence – The 'Email Deputy' System

There may be occasions when it is necessary for MPQC to access an individual's email account in their absence, in order to continue efficient operations within the organisation (e.g., where the individual has not had an opportunity to set up an 'out of office' message or redirect their email due to unplanned absence).

Dissemination of Document

Following approval by MPQC General Manager Shared Services this policy will be uploaded onto MPQC's shared drive for all employees to access.

References

References to Standards

- BS ISO/IEC 27001, British Standards for Information Security

Legislation

- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1998
- Data Protection Act 1998
- Electronic Communication Act 2000
- Freedom of Information Act 2000

Prepared:	October 2021
Version:	1.0
Approved by:	General Manager Shared Services
Review Date:	October 2023