Information Security Policy

INFORMATION SECURITY POLICY

Introduction

Mineral Products Qualifications Council (MPQC) is a 'not for profit' membership organisation whose members are derived from the quarrying, mineral products, mining, construction and related manufacturing sectors. MPQC members cover a wide breadth of the mineral products industry and range from sole traders to multi-national corporations.

Different divisions of MPQC look after information processing as a fundamental part of its purpose of providing training and qualifications for the Industry. It is important, therefore, that the organisation has a clear and relevant Information Security Policy. This is essential to our compliance with data protection and other legislation and to ensuring that confidentiality is respected.

The purpose of MPQC's Information Security policy is to protect, to a consistently high standard, all information assets. The policy covers security which can be applied through technology but perhaps more crucially it encompasses the behaviour of the people who manage information on a daily basis.

Information security is about peoples' behaviour in relation to the information they are responsible for, facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way
- Assurance that MPQC is providing a secure and trusted environment for the management of information used in delivering its business
- Clarity over the personal responsibilities around information security expected of staff when working on MPQC business
- Assurance that information is accessible only to those authorised to have access

Scope of Policy

Staff of the following areas are within the scope of this document:

- Permanent staff
- Secondees
- Contractors
- Temporary staff

Purpose of Policy

The aim of MPQC's Information Security Policy is to preserve:

Confidentiality	Access to Data shall be confined to those with appropriate authority.
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
Availability	Information shall be available and delivered to the right person, at the time when it is needed.

Roles and Responsibilities

The information within scope includes:

Chief Executive Officer
Responsibility for information security resides ultimately with the Chief Executive. This responsibility is discharged through the designated roles of Data Protection Officer (DPO).

Data Protection Officer (DPO)
MPQC has an appointed Data Protection Officer under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters. The DPO reports to the CEO and directly to the Board in relation to data protection matters.

General Managers (GM)
General Managers are responsible for the security of their physical environments where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures and user obligations applicable to their area ofwork.
- Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities for information security.
- Determining the level of access to be granted to specific individuals Ensuring staff have appropriate training for the systems they are using. Ensuring staff know how to access advice on information security matters.

All Staff
All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular all staff should undertake Data Security Awareness training as requested by the DPO and understand:

- What information they are using, how it should be protectively handled, stored and transferred.
- What procedures, standards and protocols exist for the sharing of information with others.
- How to report a suspected beach of information security within the organisation.
- Their responsibility for raising any information security concerns with the Data Protection Officer.

Contracts with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub- contractors of the external organisation comply with all appropriate security policies.

Policy Framework

Contracts of Employment
Staff security requirements shall be addressed upon appointment and all contracts of employment are governed by the staff handbook which contains the appropriate information security clause.

IT Support Company
MPQC contracts an IT Support Company (Octavian) whose contract covers maintaining security (Fire Walls, Antivirus, Anti Malware etc) and authorisation of users in line with company requirements.

Access Controls
Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant GM.

Computer and Application Access Controls
Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

Equipment Security
In order to minimise loss of, or damage to, all assets, MPQC has ensured that all electronic equipment and assets have been; identified, registered and physically protected from threats and environmental hazards.

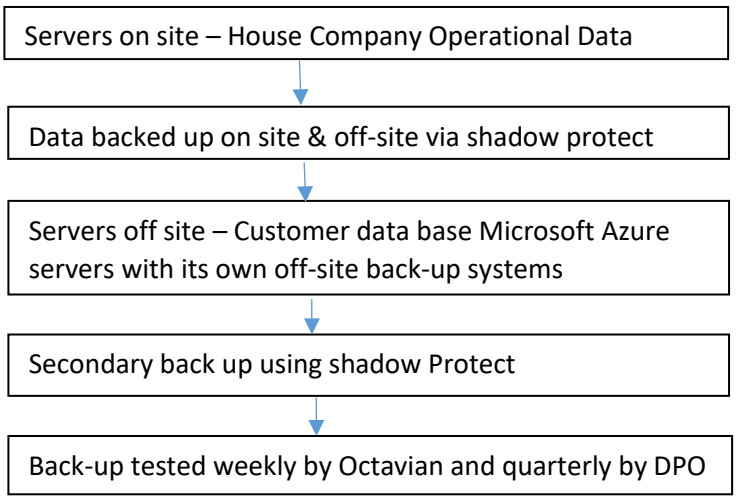
Information Security Events and Weaknesses
All MPQC information security events, near misses, and suspected weaknesses are to be reported to the Data Protection Officer. Information Security Incident Reporting procedures must be complied with.

Protection from Malicious Software
Octavian use software countermeasures and management procedures to protect MPQC against the threat of malicious software. MPQC staff shall not install software on the organisation's property without permission from the Data Protection Officer.

Monitoring System Access and Use
An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. MPQC will put in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy.

Any monitoring will be undertaken in accordance with the relevant acts and the Human Rights Act and any other applicable law.

Business Continuity and Disaster Recovery Plans
MPQC has a relevant business continuity and disaster recovery plan.



Monitoring

Compliance with this policy will be monitored via our Data Protection Officer (DPO).
The DPO is responsible for the monitoring, revision and updating of this document on a 3-yearly basis, or sooner if the need arises.

Related Policies

As well as this policy you can gain access to our Privacy Policy and Data Protection Policy by going on the MPQC website; www.mp-qc.org

Prepared:	Oct 2020
Version:	1
Approved by:	GM Shared Services
Date:	Oct 2020