DataSQRL

# Information
# Security Policy

Matthias Broecheler, Chief Executive Officer
August 2024
v1.0

# Contents

## History

| Date | Author | Description |
|---|---|---|
| 08/2024 | Matthias Broecheler | v1.0 |
| | | |
| | | |
| | | |

# 1 Introduction

Managing information is an important component of IT governance which spans information about staff, the organization, and customer information. This document describes DataSQRL's information security policy.

# 2 Objectives, Aim and Scope

## 2.1 Objectives

The objectives of DataSQRL's Information Security Policy are 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.

## 2.2 Policy Aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications, and networks owned or held by DataSQRL by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organization.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their responsibilities.
- Creating and maintaining within the organization a level of awareness of the need for Information Security as an integral part of the day-to-day business.
- Protecting information assets under the control of the organization.

## 2.3 Scope

This policy applies to all information, information systems, networks, applications, locations, and users of DataSQRL or supplied under contract.

# 3 Responsibilities

3.1 The ultimate responsibility for information security rests with the Chief Executive Officer of DataSQRL, but on a day-to-day basis the Chief Technology Officer shall be responsible for managing and implementing the policy and related procedures.

3.2 All DataSQRL employees are aware of how to access advice on information security matters.

3.3 All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action including termination.

3.4 The Information Security Policy shall be maintained, reviewed and updated by DataSQRL's co-founders. This review shall take place annually.

3.5 Each member of staff shall be responsible for the operational security of the information systems they use.

3.6 Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

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

# 4 Policy Framework

## 4.1 Management of Security

- At the board level, responsibility for Information Security shall reside with the Chief Executive Officer.
- DataSQRL's Chief Technology Officer shall be responsible for implementing, monitoring, documenting and communicating security requirements for DataSQRL.

## 4.2 Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- Ongoing awareness shall be established and maintained to ensure that staff awareness is refreshed and updated as necessary.

## 4.3 Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

## 4.4 Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

## 4.5 User Access Controls

Access to information shall be restricted to authorized users who have a bona-fide business need to access the information.

## 4.6 Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorized users who have a legitimate business need e.g., systems or database administrators. Authorization to use an application shall depend on the availability of a license from the supplier.

## 4.7 Equipment Security

To minimize loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards and locked when left unsupervised. All procurement of hardware and software used for work activities must be approved by DataSQRL's Chief Technology Officer.

All computer hardware being returned to DataSQRL's Chief Technology Officer must be properly reformatted to remove sensitive data and licensed software.

## 4.8 Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of DataSQRL's risk management program. These reviews shall help identify areas of continuing best practice and possible weaknesses, as well as potential risks that may have arisen since the last review was completed.

## 4.9 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported to the Chief Technology Officer. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

## 4.10 Classification of Sensitive Information

The classification **DataSQRL Confidential** - shall be used for customer records, customer identifiable information passing between DataSQRL staff. Documents marked DataSQRL Confidential not in a safe store or in transport should be kept out of sight of visitors or others not authorized to view them. Confidential customer data in electronic form should be sanitized of employee-specific information when used for testing purposes.

The classification **DataSQRL Restricted** - shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

- Adversely affect the reputation of the organization or its officers or cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness of the organization;
- Cause monetary loss or loss of earning potential or facilitate improper gain or disadvantage for individuals or organizations;
- Prejudice the investigation or facilitate the commission of crime or other illegal activity;
- Breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- Breach statutory restrictions on disclosure of information;
- Disadvantage the organization in commercial or policy negotiations with others or undermine the proper management of the organization and its operations.

DataSQRL Restricted documents should also be stored in a secure location.

## 4.11 Protection from Malicious Software

The organization shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy.

### 4.12 User Media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of Chief Technology Officer before they may be used on DataSQRL systems. Such media must also be fully virus-checked before being used on the organization's equipment.

### 4.13 Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed.

### 4.14 System Change Control

Changes to information systems, applications, or networks shall be reviewed and approved by the Chief Technology Officer.

### 4.15 Intellectual Property Rights

The organization shall ensure that all information products are properly licensed and approved by the Chief Technology Officer. Users shall not install software on the organization's property without permission from the Chief Technology Officer.

### 4.16 Business Continuity and Disaster Recovery Plans

The organization shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

### 4.17 Reporting

The Chief Technology Officer shall keep the Chief Executive Officer informed of the information security status of the organization by means of regular reports and presentations.

### 4.18 Human Resources Security

Prior to employment, candidates will be informed of DataSQRL security policies as they relate to customer data. Background checks are required for all new employees and upon the first week of employee and prior to receiving access to corporate resources, DataSQRL information security policies will be reviewed.

In the event where employment at DataSQRL is terminated, all physical assets must be immediately returned. Email access will be immediately revoked in addition to access to any company network and computing resources.

### 4.19 Further Information

Further information and advice on this policy can be obtained from:

Matthias Broecheler
Chief Executive Officer
Email: info@datasqrl.com
Phone: (206) 657-6576