**CUSTOMER NAME**

Information Security - Policy

Table of Contents

[1. Purpose 2](#_Toc117586850)

[2. Scope 2](#_Toc117586851)

[3. Information Security Policy 2](#_Toc117586852)

[3.1 Principle 2](#_Toc117586853)

[3.2 Chief Executive Statement of Commitment 2](#_Toc117586853)

[3.3 Introduction 3](#_Toc117586855)

[3.4 Basic information security technology 3](#_Toc117586857)

[4. Information Security Objectives 3](#_Toc117586860)

[4.1 Reference Documents (Not-employee facing) 4](#_Toc117586853)

[4.2 Reference ISMS Policies and Procedures 4](#_Toc117586853)

[5. Information Security Policy Framework 4](#_Toc117586861)

[6. Information Security Roles and Responsibilities 5](#_Toc117586861)

[7. Legal and Regulatory Obligations 5](#_Toc117586861)

[8. Training and Awareness 5](#_Toc117586861)

[9. Policy Communication and Exceptions 6](#_Toc117586861)

[10. Validity and Document Management 6](#_Toc117586861)

# **Purpose**

The aim of this top-level policy is to define the purpose, direction, principles, and basic rules for information security management. It also sets out the information security policies that apply to Customer Name to protect the Confidentiality, Integrity, and Availability of data.

# **Scope**

This Policy is applied to the entire Information Security Management System (ISMS), as defined in the ISMS Scope Document.

Users of this document are all employees of Customer Name, as well as relevant external parties.

# **Information Security Policy**

## 3.1 Principle

Information Security is managed based on risk, legal and regulatory requirements, and business need.

## 3.2 Chief Executive Statement of Commitment

In the era of changing technology and new sophisticated ways in which systems are getting compromised, information security has become a vital need of business. In order to provide an organisation-wide approach to information security DataGuard has decided to adopt ISO 27001:2013, which is the international standard for implementing and maintaining an Information Security Management System (ISMS). We have provided adequate resources and expertise to ensure that our Information Security Management system (ISMS) is continually improving to always meet the requirements of our fast-paced company.

CEO Name

Co-Founder/Co-CEO

## Introduction

Information security protects our most critical assets and all information that is entrusted to us.

An effective ISMS means that we can:

* Continually monitor information security risk.
* Demonstrate that data is processed in a manner that ensures appropriate security of the personal data.
* Maintain a standard organisational wide approach to Information Security

## 

## Basic information security terminology

**Confidentiality** – characteristic of the information by which it is available only to authorised persons or systems.

**Integrity** – characteristic of the information by which it is changed only by authorised persons or systems in an allowed way.

**Availability** – characteristic of the information by which it can be accessed by authorised persons when it is needed.

**Information security** – preservation of confidentiality, integrity, and availability of information.

**ISMS (Information Security Management System)** –part of overall management processes that take care of planning, implementing, maintaining, reviewing, and improving information security.

**ISO 27001:2013** –specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization.

# **Information Security Objectives**

The information security management system is built upon an information security policy framework. In conjunction with this policy, the following policies make up the policy framework:

## 4.1. Reference documents (not employee facing):

* ISO/IEC 27001:2013 standard, clauses 5.2 and 5.3 (not employee facing)
* ISMS Scope Document (not employee facing)
* Risk Assessment and Risk Treatment Methodology (not employee facing)
* Statement of Applicability (not employee facing)
* List of Legal, Regulatory and Contractual Obligations (not employee facing)

## 4.2. Reference ISMS Policies & Procedures (employee facing)

* Information security policy (this policy)
* Mobile device policy
* Working from home policy / teleworking
* Access control policy
* Password policy
* Acceptable use of information assets policy
* Clear desk and clear screen policy
* Backup policy
* Information classification policy
* Physical security / working in secure areas policy
* Information security incident management procedures
* Business continuity policy

# **Information Security Roles and Responsibilities**

Information security is the responsibility of each one of us at Company Name. It is the personal responsibility of you to understand and adhere to the policies, follow procedures, and to report all suspected or actual personal data breaches or security incidents.

Specific roles and responsibilities for the running and operation of the Information Security Management System are defined and recorded in the Company Name Roles and Responsibilities Matrix document.

1. **Monitoring**

Compliance with the policies and procedures of the ISMS are monitored via the ISO 27001 Management Review Team and the ISO (Information Security Officer). An independent review will also be conducted by both Internal and External parties where ISMS audits will be completed on a periodic basis.

1. **Legal and Regulatory Obligations**

* Data Protection Act 2018
* UK GDPR
* EU GDPR
* Privacy and Electronic Communications Regulations 2011 (as amended)
* Computer Misuse Act 1990
* Malicious Communications Act 1988

1. **Training and Awareness**

Policies are made readily and easily available to all employees via the Customer Name Code of Conduct/ISMS Security Manual/Employee Handbook. Other policies marked with the classification label of ‘PUBLIC’ may be shared with third-party users.

A training and communication plan is in place to communicate the policies, processes, and concepts of information security. Training needs have been identified, and relevant training requirements documented. At least once annually, all Customer Name employees are required to complete all security awareness training via our Customer Name Academy. All new joiners are required to complete all security awareness training via our Customer Name Academy as part of company onboarding.

1. **Policy** **Communication** **and** **Exceptions**

The Information Security Officer must ensure that all employees, contract staff as well as appropriate external parties are familiar with this Policy. Any exception to the policy must be approved and recorded by the Information Security Officer in advance and reported to the ISO 27001 Management Review Team.

1. **Validity** **and** **Document** **Management**

This document is valid as of Date

The owner of this document is the Information Security Officer, who must check and, if necessary, update the document at least once a year.

**Job title**

Information Security Officer

**Signature**

|  |
| --- |
| Logo  Description automatically generatedProvided by |