# Information Security Policy

Cera Care Technology

---

## Document Contents Page

# 1 Information Security Policy

## 1.1 Purpose

The purpose of this policy is to define Cera Care Technology's approach to managing information security and to establish the principles and framework for the Information Security Management System (ISMS). This policy supports the consistent application of information security controls across the Cera Care group while ensuring the protection of the confidentiality, integrity, and availability of information within the defined ISMS Scope.

## 1.2 Scope

The Information Security Policy applies to Cera Care Technology and supports the Information Security Management System (ISMS) established for it. It applies to all personnel and third parties operating on behalf of Cera Care Technology.

Cera Care operates as a group with shared management, systems, and processes. Information security controls, policies, and procedures are defined and managed at group level and formally adopted by Cera Care Technology as part of its ISMS. Other Cera Care group entities may adopt this policy where appropriate.

Responsibility for this policy and the ISMS rests with the top management of Cera Care Technology, who form part of the wider group leadership.

## 1.3 Principle

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

## 1.4 Senior Leadership Statement of Commitment

*The Senior Leadership Team affirms its commitment to establishing, maintaining and continually improving an effective Information Security Management System (ISMS). As Cera Care Technology's core services support highly vulnerable service users, we recognise that protecting their personal information is fundamental to their safety, dignity, and trust in our company. We are committed to ensuring that all information relating to service users is collected, processed, stored, and shared in a secure and responsible manner. We understand that the security of this information depends on the quality of the technology we design and operate. By building systems that are secure by design and managed responsibly throughout their lifecycle, we create the conditions necessary to keep information safe.*

*To uphold these responsibilities and achieve the intended outcome of the ISMS, the Senior Leadership Team commits to:*

- *Satisfying applicable information security requirements*
- *Integrating information security requirements into organisational processes including how we design, develop, procure and operate our technology*
- *Providing the resources necessary for an effective ISMS, including competent people, secure technologies, training and funding*
- *Communicating the importance of information security and compliance with the ISMS, ensuring employees and third parties understand their requirements and roles*
- *Promoting and reinforcing a culture of security, enabling employees and third parties to make responsible decisions*
- *Continually improving the ISMS*

04/02/2026, General Counsel

## 1.5 Introduction

Information security safeguards the data entrusted to us. When it's compromised, the consequences can be severe, impacting our employees, customers, reputation, and financial stability. By implementing an effective Information Security Management System (ISMS), we can:

- Demonstrate compliance with legal, regulatory, and contractual obligations
- Ensure the right individuals have timely and appropriate access to the right data
- Protect personal data in accordance with GDPR and other relevant regulations and requirements
- Uphold our responsibility as ethical data stewards and a trusted custodian

## 1.6 Information Security Objectives

Information Security Objectives are reviewed at least annually or when significant changes occur to the organisation. Objectives are reviewed by the Management Review Team and signed off. Objectives are based on business requirements, requirements from interested parties as well as risk.

The Information Security Objectives directly support Cera Care’s mission to empower people to live longer, better lives in their own homes through the power of technology.

Cera Care Technology’s Information Security Objectives, addressed by the ISMS, read as follow:

- To protect information assets and supporting systems by implementing and continually improving appropriate security controls
- To meet legal, regulatory and contractual obligations for information security
- To effectively manage third parties to reduce potential information security risk from suppliers
- To ensure the provision of necessary resources for effectively managing Information Security and the Information Security Management System (ISMS), addressing risks through structured risk management, and driving continual improvement
- To cultivate a security-conscious workplace through continuous education and targeted awareness initiatives

## 1.7 Information Security Defined

Information security is defined as preserving:

| | |
|---|---|
| **Confidentiality** | Ensuring that data is accessed only by authorised people |
| **Integrity** | Protecting data from unauthorised modification to ensure accuracy and trustworthiness |
| **Availability** | Making sure data and systems are accessible when needed by authorised users |

***In other words, Information Security means that the right people have the right access to the right data at the right time.***

## 1.8 Information Security Framework

This policy is supported by a framework of topic-specific policies, procedures and controls that are developed at the Cera Care group level and implemented across all Cera Care entities. The framework addresses areas including:

- Risk Management
- Acceptable Use
- Access Control
- Asset Management
- Information Classification and Handling
- Data Protection
- Mobile Devices and Teleworking
- Business Continuity
- Malware and Patching
- Change Management
- Third Party Supplier Security
- Network Security Management
- Secure Development

- Incident Management
- Continual Improvement

## 1.9 Information Security Roles and Responsibilities

It is the responsibility of everyone to understand and adhere to Cera Care's information security policies including reporting suspected or actual breaches. Specific roles and responsibilities for the running of the ISMS are defined and recorded.

## 1.10 Monitoring

Compliance with the policies and procedures of the information security management system are monitored via the Management Review Team, together with independent reviews by both Internal and External Audits on a periodic basis.

## 1.11 Legal and Regulatory Obligations

The organisation takes its legal and regulatory obligations seriously and these requirements are recorded.

## 1.12 Training and awareness

Policies are made readily and easily available to all employees and third-party users as needed. A communication plan is in place to communicate the policies, processes, and concepts of information security. Training needs are identified, and relevant training requirements are captured.

## 1.13 Continual Improvement of the Management System

The information security management system is continually improved. The continual improvement policy sets out the approach to continual improvement.

# 2 Policy Compliance

## 2.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## 2.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

## 2.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 2.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.