Heresafe Ltd, DMC02, County Way, Barnsley, S70 2AG
https://heresafe.com | hello@heresafe.com | 01226 212056

INFORMATION SECURITY POLICY

High level Information Security Policy to provide an outline and justification for risk-based information security management.

Document Control

Version:	8.0
Owner:	Daryl Greensill
Last updated:	24/02/2025
Reviewed by:	Paula Casterton
Reviewed date:	24/02/2025
Classification:	Public

Contents

Contents....2
1. Policy Details....3
1.1. Purpose....3
1.2. Scope....3
1.3. Principle....3
1.4. Information Security Defined....3
1.5. Policy Statement....4
1.5.1. Access Control Policy....4
1.5.2. Backup Policy....4
1.5.3. Bring your Own Device Policy....4
1.5.4. Business Continuity Plan....4
1.5.5. Change Management Policy....4
1.5.6. Clear Desk Clear Screen Policy....5
1.5.7. Data Classification, Labelling & Handling Policy....5
1.5.8. Disposal of Equipment Policy....5
1.5.9. Encryption Policy....5
1.5.10. GDPR: Privacy & Data Protection Policy....5
1.5.11. Information Risk Assessment Policy....5
1.5.12. Information Security Roles & Responsibilities Policy....6
1.5.13. IT Usage Policy....6
1.5.14. Mobile and Remote Working....6
1.5.15. Password Policy....6
1.5.16. Removable Media Policy....6
1.5.17. Secure Development and Deployment Policy....6
1.5.18. Supplier Security Policy....7
1.6. Legal and Regulatory Obligations....7
1.7. Training and Awareness....7
1.8. Continual Improvement of the Information Security Management System....7
2. Policy Compliance....8
2.1. Compliance Measurement....8
2.2. Exceptions....8
2.3. Non-Compliance....8
2.4. Continual Improvement....8
3. Version History....9

1. Policy Details

1.1. Purpose

Information security protects the information that is entrusted to us. Getting information security wrong can have significant adverse impacts on our employees, our customers, our reputation, and our finances.

By having an effecting information security management system, we can:

- Provide assurances for our legal, regulatory, and contractual obligations
- Ensure the right people, have the right access to the right data at the right time
- Provide protection of personal data as defined by the GDPR
- Be good data citizens and custodians

1.2. Scope

All employees and third party users.
All company information and physical assets.

1.3. Principle

Heresafe is committed to operating an Information Security Policy where:

- Risks are identified, managed, and treated according to the agreed risk tolerance.
- Authorised users can securely access and share information to perform their roles.
- Physical, procedural, and technical controls to balance user experience and security.
- Contractual and legal obligations are met and exceeded.
- Individuals accessing our information are aware of their responsibilities.
- Incidents affecting our information assets are resolved and learnt from.
- To continually improve the ISMS

1.4. Information Security Defined

Information security is defined as preserving:

Confidentiality	Access to information is to those with appropriate authority.	The right people. with the right access
Integrity	Information is complete and accurate.	to the right data,
Availability	Information is available when it is needed	at the right time.

1.5. Policy Statement

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:

1.5.1. Access Control Policy

Access to all information will be controlled and driven by business requirements. Access will be granted based on an individual's role and classification of information, only to a level which will allow them to carry out their duties.

For more information see the **Access Control Policy**.

1.5.2. Backup Policy

To maintain integrity and availability of information it is important that all information is securely backed up in case of accidental or malicious damage. The backup process should ensure that information is securely stored while minimising the impact to users.

For more information see the **Backup Policy**.

1.5.3. Bring your Own Device Policy

When you use your own device as a work tool, you must maintain the security of the Company's information you handle. This policy covers the use of personal and none Heresafe owned/issued electronic devices which could be used to access Heresafe systems and data.

For more information see the **Bring your own Device Policy**.

1.5.4. Business Continuity Plan

The Business Continuity Plan aims to assess risks and plan for crisis mitigation across all areas of the business. The plan includes several previously identified scenarios and the plans relevant to mitigate each of them.

For more information see the **Business Continuity Plan**.

1.5.5. Change Management Policy

Change Management provides a process to apply changes, upgrades, or modifications to Heresafe's operational procedures or infrastructure. The change management process attempts to identify and put in place controls to minimise risk.

For more information see the **Change Management Policy**.

1.5.6. Clear Desk Clear Screen Policy

A clear desk, clear screen will help ensure that all sensitive/confidential materials are removed from workspaces and locked away when the items are not in use or an employee leaves their workstation.

For more information see the **Clear Desk, Clear Screen Policy**

1.5.7. Data Classification, Labelling & Handling Policy

This policy will classify its information assets and the relevant controls that should be used when handling information contained within those assets. In addition, it also covers where the information is to be labelled.

For more information see the **Data Classification, Labelling & Handling Policy**

1.5.8. Disposal of Equipment Policy

This document outlines the disposal of equipment it is published to give a clear understanding of Heresafe's policy in the areas of IT equipment disposal and re-using of all other equipment, furniture, and assets.

For more information see the **Disposal of Equipment Policy**

1.5.9. Encryption Policy

Where appropriate all sensitive information should be encrypted to protect confidentiality, authenticity and integrity of information.

For more information see the **Encryption Policy**.

1.5.10. GDPR: Privacy & Data Protection Policy

This document details the privacy & data protection for products and services provided to our clients and for our sales & marketing activities.

For more information see the **GDPR Privacy & Data Protection Policy**

1.5.11. Information Risk Assessment Policy

All individuals have a duty to assess information risks by looking at the asset, the vulnerability (ease which an asset can be exploited) and the threat (the likelihood of this happening). All risks should be recorded in the Risk Treatment Plan.

For more information see the **Information Risk Assessment Policy**

1.5.12. Information Security Roles & Responsibilities Policy

This policy outlines the roles and responsibilities for the implementation, management support and ongoing review and improvement of the HereSafe Information Security Management System.

For more information see the **Information Security Roles & Responsibilities Policy**

1.5.13. IT Usage Policy

Users have a responsibility to promote IT security and must safeguard the electronic information and systems within their care and use. The IT Usage Policy defines responsibilities, restrictions and controls to ensure that all systems retain security and integrity.

For more information see the **IT Usage Policy**.

1.5.14. Mobile and Remote Working

This policy applies to the guidelines that employees must follow when working mobile or remotely must ensure that they work in a security and authorised manner.

For more information see the **Mobile and Remote Working Policy.**

1.5.15. Password Policy

Passwords are the primary method of user authentication. The password policy defines best practice to how users should create and use passwords to minimise risk of account credentials being compromised.

For more information see the **Password Policy**.

1.5.16. Removable Media Policy

This policy is intended to outline responsibilities and controls around the use of removable media. Removable media refers to any type of computer storage that is not physically fixed inside a computer.

For more information see the **Removable Media Policy.**

1.5.17. Secure Development and Deployment Policy

As a software developer it is vitally important that all software development and deployments are done in a secure manner. The Secure Development and Deployment Policy identifies best practices that should be followed in every element of software development.

For more information see the **Secure Development and Deployment Policy**.

1.5.18. Supplier Security Policy

Security should be considered when establishing relationships with suppliers to ensure security is maintained through the entire supply chain. The Supplier Security policy defines a set of controls for selecting and working with suppliers.

For more information see the **Supplier Security Policy.**

1.6. Legal and Regulatory Obligations

Heresafe takes its legal and regulatory obligations seriously and these requirements are recorded in the **Information Security Legal Compliance Register**.

1.7. Training and Awareness

Policies are made readily and easily available to all employees and third-party users. A training and communication plan is in place to communicate the policies, process, and concepts of information security.

1.8. Continual Improvement of the Information Security Management System

The information security management system is continually improved. The **Continual Improvement Policy** sets out the company approach to continual improvement and there is continual improvement process in place.

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.

3. Version History

Version	Date	Author	Notes
1.0		Daryl Greensill	New Policy
2.0 - 5.0		Daryl Greensill	Historical updates
6.0	18/02/2021	Paula Casterton	Addition of policies which fall within the ISMS.
7.0	12/05/2021	Paula Casterton	Addition of objectives to continually improve the ISMS. Information Handling Policy has now been archived as it forms part of the Data Classification, Labelling & Handling Policy.
7.1	12/04/2023	Daryl Greensill	Minor wording changes to: - Bring your own Device Policy - Change Management
8.0	24/02/2025	Daryl Greensill	Change to Heresafe branding and new template.