INFORMATION SECURITY POLICY

CFH Docmail Ltd.
Tel: 01761 416311 • **Email:** info@cfh.com • **Web:** cfh.com • St Peter's Park, Wells Road, Westfield, Radstock, BA3 3UP
Registered in England No. 1716891 • VAT Reg. No. GB 720 9782 23

CFH DOCMAIL LIMITED – INFORMATION SECURITY POLICY

The Board of Directors and management of CFH Docmail Limited (including Print For Business Limited) are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organisation.

This policy applies to all CFH Docmail Limited (including Print For Business Limited) sites, employees, contractors and visitors. The purpose of this policy is to ensure that staff and customers understand CFH Docmail Ltd Information Security requirements.

CFH Docmail Limited is committed to achieving and maintaining certification of its ISMS to ISO 27001:2013 incorporating C&CCC Standard 55 and C&CCC Standard 3(CPAS Rules) and compliance with the GDPR and the Data Protection Act 2018 (as re-enacted or amended).

The Standards and Regulations detailed above provide a framework for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS.

All Employees of CFH Docmail Limited are expected to comply with this policy and with the ISMS that implements this policy. All Employees will receive appropriate training as specified in the CFH Docmail Limited Group Training and Education Policy. The consequences of breaching the information security policy are set out in the disciplinary policy contained within the Staff Handbook and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

In this Policy, Information Security is defined as:

Preserving the availability, confidentiality and integrity of the physical (assets) and information assets. This is expanded on below.

Preserving
This means that management, all full time or part time Employees, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. All Employees will receive information security awareness training and more specialised Employees will receive appropriately specialised information security training (such as DPO's and Information Security Auditors).

CFH Docmail Ltd.
Tel: 01761 416311 • **Email:** info@cfh.com • **Web:** cfh.com • St Peter's Park, Wells Road, Westfield, Radstock, BA3 3UP
Registered in England No. 1716891 • VAT Reg. No. GB 720 9782 23

the availability
This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and CFH Docmail

Limited must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

confidentiality
This involves ensuring that information is only accessible to those authorised to access it and therefore to prevent both deliberate and accidental unauthorised access to CFH Docmail Limited information and proprietary knowledge, and its systems.

and integrity
This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data.

There must be appropriate contingency including for network(s), e-commerce system(s), website(s),extranet(s) and data backup plans and security incident reporting. CFH Docmail Limited must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)
The physical assets of CFH Docmail Limited including, but not limited to, buildings, equipment, people, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and information assets
The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.) CFH Docmail Limited current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of certification to ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are

CFH Docmail Ltd.
Tel: 01761 416311 • **Email:** info@cfh.com • **Web:** cfh.com • St Peter's Park, Wells Road, Westfield, Radstock, BA3 3UP
Registered in England No. 1716891 • VAT Reg. No. GB 720 9782 23

fundamental to this policy. Control objectives for each of these areas are supported by specific documented policies and procedures.

CFH Docmail Limited aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

This means that management, all full time or part time Employees/Staff, sub-contractors, project consultants and any relevant external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS.

CFH Docmail Limited undertakes annual review of business objectives and performance in order to improve the way we protect and manage our business and information assets to enable us to meet contractual, legislative, privacy, ethical responsibilities and strategic aims.

We will identify security risks and their relative priorities, responding to them promptly and implementing safeguards that are appropriate, effective, culturally acceptable and practical.

CFH Docmail Limited works proactively with our Customers to identify and deliver continuous improvements to systems, documents and management information in order to enhance both the Company and the Customer's business processes.

A current version of this document is available to all members of staff on the corporate network, noticeboards and websites. It does not contain confidential information and can be released to relevant external parties.

Bill McFedries
CFH Docmail Limited
Group Managing Director/CEO

CFH Docmail Ltd.
Tel: 01761 416311 • **Email:** info@cfh.com • **Web:** cfh.com • St Peter's Park, Wells Road, Westfield, Radstock, BA3 3UP
Registered in England No. 1716891 • VAT Reg. No. GB 720 9782 23