Information Security Policy

1.0 Purpose

Information is a major asset that Changefirst has a responsibility and requirement to protect.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Changefirst maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

We have carefully assessed and ensured all the requirements as identified by information owners and clients, for the maintaining confidentiality, integrity and availability of information assets and processing facilities required for operation activity shall be met.

This Information Security Policy addresses all these areas to ensure the confidentiality, quality and availability of information. The following policy details the basic requirements and responsibilities for the proper management of information assets at Changefirst. The policy specifies the means of handling and transferring information within the Business.

2.0 Policy Objectives

- To direct the design, implementation and management of an effective Information Security Management System (ISMS), which ensures that Changefirst's information assets are properly identified, recorded, and afforded suitable protection at all times.
- To ensure the confidentiality, integrity, and availability of Changefirst's information assets, and supporting assets (including information systems) as defined within the Inventory of Assets.
- To ensure that all vulnerabilities, threats and risks to information assets and supporting assets are formally identified, understood, assessed and controlled in accordance with Changefirst's documented Risk Assessment Methodology.
- To ensure that Changefirst's employees, contractors and third-party users comply with this Information Security Policy, and all other ISMS documentation, through the provision of effective information security training, awareness and ongoing monitoring activities.
- To ensure that Changefirst is able to maintain full compliance with all applicable legislation, regulations and contractual requirements., and any supporting management system certifications (for example ISO/IEC 27001:2013).

3.0 Policy Scope

Changefirst's Information Security Policy shall include the following:

3.1 **Information Assets**

All information assets (data) either owned by Changefirst or entrusted to Changefirst by a client under an agreement which specifically details Changefirst's responsibility for that data, and including:

- Information assets held, processed or stored on Changefirst premises
- Information assets held, processed or stored at approved off-site premises or locations

3.2 Supporting Assets

All supporting assets (non-data) which by direct or indirect association are an integral part of ensuring the confidentiality, integrity or availability of the information assets described in Section 2.1, including:

- Premises (including offices, factories, data centres, storage facilities, recovery sites etc.)
- Hardware (including servers, network infrastructure, laptop computers, desktop computers, storage infrastructure and mobile devices)
- Software (including operating systems, commercially available software applications and software applications developed internally by Changefirst)
- Changefirst personnel (including permanent, temporary, full-time and part-time employees, authorised contractors and any third-party users of information systems)

3.3 Documentation and Records

All policies, processes, procedures, work instructions and records related to the management, use, control and disposal of the information assets and their supporting assets detailed above.

4.0 Policy Statements

Changefirst shall be committed to the protection of the information assets and supporting assets as defined within the Scope of this Policy. Changefirst has created its Information Security Management System (ISMS) in accordance with the international Information Security Management Systems standard ISO/IEC 27001:2013: this framework shall be followed for all information security related activities.

To effectively manage and deliver its ISMS, Changefirst shall:

4.1 Inventory of Assets

Define and maintain a comprehensive Inventory of Assets, including all information assets and supporting assets as defined within Section 2.0 of this Policy. The Inventory of Assets shall detail a named owner for each asset, who will fully understand their responsibilities for the protection of the asset in accordance with the documented Changefirst Asset Management Policy.

4.2 Access Control Policy

Ensure that all information assets, and their supporting assets, are protected so as to ensure their confidentiality, integrity and availability is maintained. Access to information assets and supporting assets shall be in accordance with Changefirst's Access Control Policy, and be restricted to the minimum required to undertake authorised business activities, and Changefirst has adopted the principle that "access is forbidden unless it has been specifically and formally pre-authorised".

4.3 Information Classification and Handling

Ensure that all information assets shall be classified and handled in accordance with the Changefirst Information Classification and Handling Guide, which details how information assets of different sensitivities shall be managed, handled, processed, encrypted, stored, transmitted, dispatched and disposed of when no longer required. This Guide also details the appropriate levels of personnel screening or clearances necessary to access information of different classifications.

4.4 Acceptable Use

Ensure that all personnel, contractors and third-party users comply with the Changefirst Acceptable Use Policy which details how information assets and their supporting assets should be used in an acceptable manner and in accordance with all ISMS related policies and processes. This policy shall detail the acceptable methods of use of information processing systems, networks (including, for example, the internet and telephone systems) and other resources within the Scope of this Policy.

4.5 Risk Assessment

Perform risk assessments on all information assets, and their supporting assets, as detailed within Changefirst's Risk Management Policy. The documented results of risk assessments shall be reviewed to understand the level of risk to information and supporting assets, and appropriate controls implemented as appropriate to address any unacceptable risks that have been identified.

4.6 Information Security Incidents

Provide a mechanism for the prompt identification, reporting, investigation and closure of information security incidents to Changefirst, in accordance with the Information Security Incident Policy, and to fully analyse reported incidents to identify the root cause of issues and take advantage of any improvement opportunities which may have been identified.

4.7 Access to Information and Systems

Ensure that an Access Control Policy is in place to protect all Changefirst networks, information systems and information assets from any unauthorised access. Legitimate remote access shall only be granted in accordance with the policy to bona-fide personnel, contractors and third-party users, and only applies to access from Changefirst approved devices. Remote connections shall be used strictly in accordance with the Acceptable Use Policy. Remote access shall be regularly reviewed and any connections that are no longer required shall be removed immediately.

4.8 Business Continuity Management

Ensure that information security is a key consideration within the Business Continuity Management Policy, so that the security of Changefirst information assets is not compromised even when faced with a wide variety of unplanned business interruptions.

4.9 Information Security Training

Develop a regular training and education programme, in accordance with the Information Security Training Policy, which shall be mandatory for all Changefirst employees, contractors and third-party users, which details their individual responsibilities to fully adhere to the requirements of the ISMS policies, processes and work instructions defined within Section 2.0 of this Policy.

4.10 Management, Monitoring and Review

Continually monitor, review and improve the Changefirst ISMS, in accordance with the Management Review Policy, by undertaking regular reviews, internal audits (in accordance with the Internal Audit Policy) and other related activities, and taking prompt corrective actions and implementing improvement opportunities in response to the findings of these activities.

4.11 Legislative Compliance

Ensure that, at all times, its Information Security Management System shall support full compliance with the following UK and EU legislation and regulations, including but not limited to:

- General Data Protection Regulation 2016
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Companies Act 1985
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Waste Electrical and Electronic Equipment Directive (WEEE) 2003

- Payment Card Industry Data Security Standard (if applicable)

5.0 Responsibilities

5.1 Employees, Contractors and Third-Party Users

Within Changefirst, all employees, contractors and third-party users shall understand their role in ensuring the security of information assets (and their supporting assets) in accordance with the Information Security Training Policy as detailed in Section 3.0.

There are, however, additional responsibilities defined in order that the Information Security Management System (ISMS) shall operate efficiently and in accordance with the requirements of ISO/IEC 27001:2013. These are detailed below.

5.2 Senior Management

The Managing Director and Senior Management Team shall be responsible for the following activities within the Changefirst ISMS:

- Agreeing the business need for this ISMS, and communicating their ongoing commitment to it
- Reviewing and signing off this Information Security Policy
- Setting and reviewing Changefirst's Information Security Objectives
- Assigning appropriate resources necessary to manage and operate the ISMS effectively
- Agreeing the level of acceptable risk within the Risk Assessment Methodology
- Approving any decisions not to address any unacceptable residual risks, where identified
- Having ultimate responsibility for actions related to information security incidents/breaches
- Overseeing any disciplinary action resulting from information security incidents/breaches

5.3 Information Security Manager

The Information Security Manager shall have functional responsibility for the Changefirst ISMS, and shall be responsible for the daily operational tasks of the ISMS, including:

- Ensuring an appropriate structure of ISMS policies, processes and work instructions
- Ensuring that appropriate records are created and maintained for all ISMS activities
- Ensuring the ISMS operates in accordance with the current requirements of ISO27001
- Arranging a programme of risk assessments, risk treatments and internal audits
- The preparation and communication of the Statement of Applicability
- The provision of an appropriate user training and awareness programme for employees

5.4 Operations Manager

The Operations Manager shall be responsible for:

- Overall management of the information security controls in production processes
- Overall management and functionality of Changefirst's business continuity plan
- The provision of a user training and awareness programme for suppliers and contractors
- The design and review of technical security controls, including Changefirst networks
- Supporting reviews, internal audits and risk assessments within their area of responsibility

5.5 Department/Function Managers

Managers within Changefirst shall be responsible for:

- Ensuring their team members are aware of and remain compliant with all information security policies, processes and work instructions, and that they receive appropriate training
- The provision of a user training and awareness programme for applicable third-party users
- Supporting reviews, internal audits and risk assessments within their area of responsibility

5.6 Asset Owners

As per the Asset Management Policy, designated Asset Owners shall be responsible for:

- Assessing the value of their asset(s) to the Company
- Undertaking detailed risk assessments on their asset(s), including the identification of controls and assessing their effectiveness (as per the Risk Assessment Methodology)
- Addressing any unacceptable risks (as per the Risk Assessment Methodology)
- Assisting in the investigation, resolution and closure of any information security incident which directly or indirectly affects the security of their asset(s)
- Reviewing and authorising the levels of access to their asset(s) which are granted to others (as per the Access Control Policy)
- Contributing to the Acceptable Use Policy, specifically for the use of their asset(s)

5.7 Control Owners

As per the **Asset Management Policy**, Control Owners shall be responsible for:

- The way in which their assigned control(s) are selected, implemented and operated
- Understanding which asset(s) are reliant upon each of their assigned controls
- Providing feedback to asset owners on the operation of each control, to assist them in undertaking accurate risk assessments of their asset(s)
- Assisting in the investigation, resolution and closure of any information security incident which actually or potentially indicates the failure of a control

6.0 Document Control

This Policy needs to be formally reviewed on an annual basis, as a minimum, or if required changes are identified to address one or more of the following:

- A change in business activities, which will or could possibly affect the current operation of the Company Information Security Management System.
- A change in the manner in which the Company manages or operates its information assets and/or their supporting assets.
- An identified shortcoming in the effectiveness of this Policy, for example as a result of a reported information security incident or an audit finding.

The current version of this Policy, together with its previous versions, shall be recorded below.

Version	Description	
1.0	Date Live:	*30/07/2016*
	Version Notes:	-
	Reviewed by:	*Istvan Orban*
	Approved by:	Nathan Brewer
1.1	Date Live:	10/03/2017
	Version Notes:	
	Reviewed by:	Donna Imrie-Browne
	Approved by:	Audra Proctor
1.2	Date Live:	21/05/2018
	Version Notes:	GDPR reference added
	Reviewed by:	Donna Imrie-Browne
	Approved by:	Clare Hayward