Information Security Policy of Foresight Cyber Ltd

Version: 1.4

Release date: 2022-04-06

Document classification: **PUBLIC**

FORESIGHT®
CYBER

OVERVIEW & CEO STATEMENT

Role of Information and Information Systems – Foresight Cyber is critically dependent on information and information systems. If important information was disclosed to inappropriate persons, the company could suffer serious losses or go out of business. The good reputation that Foresight Cyber enjoys is also directly linked with the way that it manages both information and information systems. For example, if private customer information were to be publicly disclosed, the organisation's reputation would be harmed. For these and other important business reasons, executive management working in conjunction with the board of directors has initiated and continues to support an information security effort. One part of that effort is definition of these information security policies.

Team Effort - To be effective, information security must be a team effort involving the participation and support of every Foresight Cyber employee who deals with information and information systems. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of users and the steps they must take to help protect Foresight Cyber information and information systems. This document describes ways to prevent and respond to a variety of threats to information and information systems including unauthorised access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

Involved Persons - Every worker at Foresight Cyber must comply with the information security policies found in this and related information security documents. Staff who deliberately violate this and other information security policy statements will be subject to disciplinary action as described in the corporate employee handbook.

Involved Systems - This policy applies to all computer and network systems owned by or administered by Foresight Cyber. This policy applies to all operating systems, computer sizes, and application systems. The policy covers information handled by computers and networks and other manifestations of information such as voice and paper. For information about the protection of information in paper form, see the Information Classification Policy [insert link here – temp as an Appendix to this policy document].

CONTENTS

INTRODUCTION

ISO27001 ISMS – This policy document format aligns to the requirements of ISO27001 Information Security Management System (ISMS), and principally follows its key Clause and controls layout. As such it assists Foresight Cyber staff in ensuring that the organisation meets its regulatory, legislative, contractual and corporate commitments to ensure the continued security of Foresight Cyber data in addition to that of its clients, partners and customers.

CLAUSE 5 – INFORMATION SECURITY POLICY

Objective

To protect potential fraud and embezzlement, industrial espionage, sabotage, errors and omissions, and system unavailability this policy ensure that all users of Foresight Cyber data / information are aware of their individual responsibilities to protect that data at all times, at all times and in all locations.

This policy document details both reasonable and practical ways for all of us at Foresight Cyber to prevent unnecessary losses.

Policy

- This information security policy applies to all staff, permanent, temporary, contractors and 3rd party partners who need to work with Foresight Cyber data, whether in hardcopy or electronic format
- To protect company information, and data entrusted into its care by Foresight Cyber's clients, all staff must bring to the attention of the Information Security Officer (ISO), any risk, weakness or failing that is discovered
- Foresight Cyber's designated ISO shall review this document at least annually - to maintain their suitability, adequacy and effectiveness - ensuring that revised copies are published and available to all staff
- Should major changes to Foresight Cyber's business model, significant technological changes or its risk approach, this policy must be reviewed for applicability

CLAUSE 6 – ORGANISATION OF INFORMATION SECURITY

Objective

To establish a management framework to initiate and control the implementation and operation of information security within the organisation.

Policy

- The CEO shall appoint an ISO, who is responsible for the day-to-day management of information security
- All information security responsibilities shall be defined and allocated
- Where necessary specific roles must be segregated to reduce opportunities for unauthorised modification or unauthorised access
- Where possible contact with special interest groups should be maintained
- Information security shall form part of all project management, regardless of the type of project

CLAUSE 7– HUMAN RESOURCE SECURITY

Objective

To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Policy

- Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks
- Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation
- There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an offence

- Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced

CLAUSE 8 – ASSET MANAGEMENT

Objective

To identify organisational assets and define appropriate protection responsibilities.

Policy

- Inventory of assets – Information, other assets associated with information and information processing facilities shall be identified and an inventory of those assets shall be drawn up and maintained
- Ownership of assets - Assets maintained in the inventory shall have an owner
- Acceptable use of assets – Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented
- Return of assets – All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment, contract or agreement
- Information classification:

To ensure that all information handled and processed by Foresight Cyber is given the appropriate protection by ensuring that its value and sensitivity is afforded to all documents, whether in hardcopy or electronic format. Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification:

- All documents shall be assigned / labelled in accordance with the data classification standard [see appropriate guidance document]
- All documents shall have an owner. Note that the author may not necessarily be the owner of a document
- Data will default to 'Not marked' if no classification is applied
- No Confidential information will be shared outside of Foresight Cyber, without the written approval of an Executive Board member
- Should information be accidentally shared with non-authorised parties, the Executive Board / ISO must be informed immediately, so that counter-compromise actions can be taken with the minimum of delay

- Additional controls and measures must be afforded to the handling and processing of personal data, frequently referred to as Personally Identifiable Information (PII), which must comply with the Data Protection Act 1998 and / or the General Data Protection Regulation (GDPR) requiring protection of EU citizen personal data
- Where possible data classification shall be tied to appropriate retention obligations
- Media handling:
- Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by Foresight Cyber
- Media shall be disposed of securely when no longer required, using formal procedures
- Media containing information shall be protected against unauthorised access, misuse or corruption during transportation
- Document redaction – prior to sharing - must follow set procedures to ensure that the censoring process cannot be reversed

CLAUSE 9 – ACCESS CONTROL

Objective

To limit access to information and information processing facilities.

Policy

- This access control policy shall be applicable to all staff, partners and 3rd party partners
- Access to networks and network services - Users shall only be provided with access to the network and network services that they have been specifically authorised to use
- User access management:
    - Users registration & de-registration – A formal registration and de-registration process shall be implemented to enable assignment of access rights
    - User access provisioning - A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services
    - Management of privileged access rights – The allocation of privileged access rights shall be restricted and controlled
    - Management of secret authentication information of users - The allocation of secret authentication information shall be controlled through a formal management process

  - Review of user access rights - Asset owners shall review users' access rights at regular intervals
  - Removal or adjustment of access rights - The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change
  - User responsibilities – Users shall be required to follow Foresight Cyber's practices in the use of secret authentication information

- System and application access control:

  - Information access restriction – Access to information and application system functions shall be restricted in accordance with the access control policy
  - Secure log-on procedures – Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure
  - Access control to program source code – Access to program source code shall be restricted

CLAUSE 10 – CRYPTOGRAPHY

Objective

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

Policy

- Policy on the use of cryptographic controls - A policy on the use of cryptographic controls for the protection of information shall be developed and implemented
- Key management - A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole life

CLAUSE 11 – PHYSICAL AND ENVIRONMENTAL SECURITY

Objective

To prevent unauthorised physical access, damage and interference to Foresight Cyber's information and information processing facilities.

Policy

- All office locations shall be subjected to a physical security controls review before Foresight Cyber's information processing facilities can operate
- Foresight Cyber's CISO will be responsible for assessing and maintaining adequate physical security controls
- Weaknesses will be reported to the CEO
- Physical controls will be examined by the CISO to ensure that they meet company's risk profile and are adequate to protect all information whether in hardcopy or electronic format for:
    - Main office
    - 'Server room' on the mezzanine floor
    - Meeting room
- The delivery and loading area will be separated from the main office
- Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access
- Staff shall be advised to take additional care when processing sensitive data whilst visitors are in the main office room
- When not in use, sensitive information must always be protected from unauthorised disclosure. When left in an unattended room, sensitive information in paper form must be locked away in appropriate containers
- Desks must be free of magnetic / removable media, and paper documents at the end of each working day
- Computer systems must invoke their security enabled screensavers automatically within 15 minutes of inactivity if not already set when the user leaves his/her desk
- All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use
- Employees must take additional care when using portable computing devices when away from main office
- Equipment, information or software shall not be taken off-site without prior authorisation

CLAUSE 12 – OPERATIONAL SECURITY

Objective

To ensure correct and secure operations of information processing facilities.

Policy

- Operational procedures and responsibilities:
    - **Documented operating procedures:** Control operating procedures shall be documented and made available to all users who need the them
    - **Change management:** Changes to Foresight Cyber, business processes, information processing facilities and systems that affect information security shall be controlled.
    - **Capacity management:** The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance
    - **Separation of development, testing and operational environments:** Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment
- **Protection from malware:** Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness
- Backup:
    - **Information backup:** Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy
    - **Logging and monitoring:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed
    - **Protection of logging information:** Logging facilities and log information should be protected against tampering and unauthorised access
    - **Administrator and operator logs:** System administrator and system operator activities shall be logged and the logs protected and regularly reviewed
    - **Clock synchronisation:** The clocks of all relevant information processing systems within Foresight Cyber shall be synchronised to a single reference time source
    - **Control of operational software:** Procedures should be implemented to control the installation of software on operational systems
- Technical vulnerability management:
    - **Management of technical vulnerabilities:** Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, Foresight Cyber's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk
    - **Restrictions on software installation:** Rules governing the installation of software by users shall be established and implemented.
- Information systems audit considerations
    - **Information systems audit controls:** Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes

CLAUSE 13 – COMMUNICATIONS SECURITY

Objective

To ensure the protection of information in networks and its supporting information processing facilities.

Policy

- Network security management:
  - **Network controls:** Networks shall be managed and controlled to protect information in systems and applications
  - **Security of network controls:** Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced
  - **Segregation in networks:** Groups of information services, users and information systems shall be segregated on networks
- Information transfer:
  - **Information transfer policies and procedures:** Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities
  - **Agreements on information transfer:** Agreements shall address the secure transfer of business information between Foresight Cyber and external parties
  - **Electronic messaging:** Agreements shall address the secure transfer of business information between Foresight Cyber and external parties
  - **Confidentiality or non-disclosure agreements:** Requirements for confidentiality or non-disclosure agreements reflecting Foresight Cyber's needs for the protection of information should be identified, regularly reviewed and documented

CLAUSE 14 – SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Objective

To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks

Policy

- Security requirements of information systems
    - **Information security requirements analysis and specification:** Information security requirements and controls shall reflect the business value of the information involved and the potential negative business impact which might result from lack of adequate security
    - **Securing application services on public networks:** Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification
    - **Protecting application services transactions:** Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay
- Security in development and support processes:
    - **Secure development policy:** Rules for the development of software and systems shall be established and applied to developments within Foresight Cyber
    - **System change control procedures:** Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures
    - **Technical review of applications after operating platform changes:** When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security
    - **Restrictions on changes to software packages:** Modifications to software packages shall be discouraged, limited to necessary changes and all changes should be strictly controlled
    - **Secure system engineering principles:** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts
    - **Secure development environment:** Foresight Cyber shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle
    - **Outsourced development:** Foresight Cyber shall supervise and monitor the activity of outsourced system development
    - **System security testing:** Testing of security functionality shall be carried out during development
    - **System acceptance testing:** Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions
- Test data:
    - Test data shall be selected carefully, protected and controlled
    - No PII is to be used for testing unless its collection for testing or design purposes explicitly states this when users' provide consent

CLAUSE 15 – SUPPLIER RELATIONSHIPS

Objective

To ensure protection of Foresight Cyber's assets that is accessible by suppliers.

Policy

- **Information security policy for supplier relationships:** Information security requirements for mitigating the risks associated with supplier's access to Foresight Cyber assets shall be agreed with the supplier and documented
- **Addressing security within supplier agreements:** All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, Foresight Cyber's information
- **Information and communication technology supply chain:** Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain
- **Monitoring and review of supplier services:** Foresight Cyber shall regularly monitor, review and audit supplier service delivery
- **Managing changes to supplier services:** Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks
- **3rd party processing of PII:** Foresight Cyber shall ensure that any external party supplier that handles or processes EU citizen data is fully compliant with the requirements of GDPR

CLAUSE 16 –INFORMATION SECURITY INCIDENT MANAGEMENT

Objective

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Policy

- Responsibilities and procedures: Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents
- Reporting information security events: Information security events shall be reported through appropriate management channels as quickly as possible
- Reporting information security weaknesses: Employees and contractors using the organisation's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services
- Assessment of and decision on information security events: Information security events shall be assessed, and it should be decided if they are to be classified as information security incidents
- Response to information security incidents: Information security incidents shall be responded to in accordance with the documented procedures
- Learning from information security incidents: Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents
- Collection of evidence: Foresight Cyber shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence

CLAUSE 17 – INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Objective

Information security continuity shall be embedded in Foresight Cyber's business continuity management systems.

Policy

- Planning information security continuity: Foresight Cyber shall determine its requirements for information security and the continuity of information security in adverse situations, e.g. during a crisis or disaster

- **Implementing information security continuity:** Foresight Cyber shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation
- **Verify, review and evaluate information:** Foresight Cyber shall verify the established and implemented information security continuity controls at regular intervals in order to ensure
- **Availability of information processing facilities:** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements

CLAUSE 18 – COMPLIANCE

Objective

To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

Policy

- **Identification of applicable legislation and contractual requirements:** All relevant legislative statutory, regulatory and contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation
- **Intellectual property rights:** Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products
- **Protection of records:** Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislatory, regulatory, contractual and business requirements
- **Privacy and protection of PII:** Privacy and protection of Personally Identifiable Information (PII) shall be ensured as required in relevant legislation and regulation where applicable
- **Regulation of cryptographic controls:** Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations
- **Independent review of information security:** Foresight Cyber's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur
- Compliance with security policies and standards: Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements

- **Technical compliance review:** Information systems shall be regularly reviewed for compliance with the organisation’s information security policies and standards

REFERENCES

The Data Protection Act 1998, UK

General Data Protection Directive, EU

ISO27001:2013

The Computer Misuse Act 1990, UK

RELATED DOCUMENTS

None

APPROVAL AND OWNERSHIP

Created By	Title	Date	Signature
Bob Mann	CISO	4th January 2021	electronic
Approved By	**Title**	**Date**	**Signature**
Vladimir Jirasek	CEO	7th January 2021	electronic

REVISION HISTORY

Version	Revision Date	Review Date	Description
V0.1- v0.4	9th May 2017		Document creation
V1.0	10th May 2017	1st May 2018	First version
V1.1	1st May 2018	30th April 2019	Review - changes
V1.2	1st May 2019	20th April 2020	Moved to a new company branded template
V1.3	7th January 2021	31st January 2022	Small corrections and styling
V1.4	6th April 2022		Changes page numbers Moved to a new company template

FORESIGHT®
CYBER

Registered address:
71-75 Shelton Street
Covent Garden
London
WC2H 9JQ
United Kingdom

Business address CZ:
Daliborova 423/19

709 00
Ostrava - Mariánské Hory
Czech Republic

Contacts:
UK Office: +44 20 8159 8942
General enquiries: info@foresightcyber.com
Finance team: finance@foresightcyber.com
Data protection Office: dpo@foresightcyber.com
Directors: directors@foresightcyber.com

https://foresightcyber.com
@foresightcyber

VAT: GB144735213
Company number: 06871193
D-U-N-S number: 211601017

DISCOVER | ASSESS | DETECT | PROTECT | RECOVER