FordHaven - Information Security Policy

Introduction

This information security policy is a key component of the FordHaven (FH) management framework. It sets the requirements and responsibilities for maintaining the security of information within FH. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

Purpose

This policy is intended to support FH business objectives and, without undue restrictions, protect its volunteers, employees, clients, contractors, third parties and the business from illegal or damaging events or actions by individuals, either knowingly or unknowingly.

The objective of this policy is to define the FH's policies that in order to protect the confidentiality, integrity and availability of FH's information assets, its reputation and the safety of all its stakeholders. Everyone who works in or with the organisation has a duty and a responsibility to comply with these policies.

Applicability

The policy applies to the use of all FH IT equipment and information systems belonging to or managed by the organisation, including but not limited to: laptops, workstations, servers, networks, supporting infrastructure, telephones, telephony systems, mobile devices (such as smart-phones), removable media, third-party systems and any cloud-based infrastructure, platforms or services.

This policy is applicable to all FH employees both permanent and temporary, volunteers, contractors, agency workers and any third parties who provide services. It is the responsibility of all such individuals to read and understand this policy, and to conduct activities in full accordance with it. If there is any uncertainty, employees should consult the centre manager.

Aim and Scope of this policy

The aims of this policy are to set out the rules governing the secure management of our FH information by:

• preserving the **confidentiality, integrity and availability** of our business information

• ensuring that all members of staff are aware of and fully comply with the relevant **legislation** as described in this and other policies

• ensuring an approach to security in which all members of staff fully understand their own **responsibilities**

• creating and maintaining within the organisation a level of **awareness** of the need for information
• detailing how to **protect** the information assets under our control

This policy applies to all information/data, information systems, networks, applications, locations and staff of FH or supplied under contract to it.

Responsibilities
Ultimate responsibility for information security rests with the Trustees but the centre managers shall be responsible for managing and implementing the policy and related procedures.
Responsibility for maintaining this Policy, the business Information Risk Register and for recommending appropriate risk management measures is held by the centre managers. Both the Policy and the Risk Register shall be reviewed by the Trustees at least annually.
Managers are responsible for ensuring that their permanent staff, volunteers temporary staff and contracts are aware of:-
• The information security policies applicable in their work areas
• Their personal responsibilities for information security
• How to access advice on information security matters

All staff and volunteers shall comply with the information security policy and must understand their responsibilities to protect FordHaven's data. Failure to do so may result in disciplinary action.
Managers shall be individually responsible for the security of information within their business area.
Each member of staff shall be responsible for the operational security of the information systems they use.
Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.
In order to ensure compliance, the following is needed:
• Appoint a Trustee with specific responsibilities for security – the risk owner;
• Appoint a person responsible for with day–to-day security;
• Identify individuals responsible for specific information assets such as: Referral / client information, staff or finance information. They need to be able to understand the threats likely to compromise the information.

• Ensure that all individuals with designated security responsibilities undertake appropriate training for their role.

Risk Assessment and Management

FH will adopt a risk assessment methodology as part of an holistic risk management approach covering all areas of protective security across its organisation. It will include a risk register (with assigned risk owners) recording any specific vulnerabilities or security risks, the control measures taken to mitigate these risks, and any adjustments over time following changes to the threat environment. Subject to security considerations, the risk register should be made widely available within the organisation to ensure all business units have an input It will include:

• A statement of the IT assets deployed by the FH – the asset register.
• A statement of the threats faced by the FH
• A statement of the impacts of compromise of the information assets
• A statement of the tolerable level of risk (the risk appetite)
• Record the application of proportionate selection of technical, procedural, personnel and physical security controls to manage the identified risks to a level that the business can tolerate;

For all projects that include the use of personal information FH must assess the privacy risks to individuals in the collection, use and disclosure of the information and a Privacy Impact Assessment (PIA) / Data Protection Impact Statement (DPIA), as recommended by the Information Commissioner, must be carried out as a minimum

Have the ability to regularly audit information assets and ICT systems to check compliance and extract data in the event of an incident;

Where shared systems or services are used, the FH must satisfy themselves that the use of these systems or services can be managed within its own risk appetite.

◦ FH is established as a private organisation limited by guarantee
◦ FH is required to abide by certain UK, European Union and international legislation.
◦ In particular, FH is required to comply with:

Legislation

• The Data Protection Act (2018)(Including GDPR)
• The Data Protection (Processing of Sensitive Personal Data) Order 2000.

• The Copyright, Designs and Patents Act (1988)
• The Computer Misuse Act (1990)

• The Health and Safety at Work Act (1974)
• Human Rights Act (1998)
• Freedom of Information Act 2000

Personnel Security

Contracts of Employment/Volunteer Agreement

• Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.
• References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity.
• Information security expectations of staff shall be included within appropriate job definitions.
• Whenever a staff member leaves the organisation their accounts will be disabled the same day they leave.

Information Security Awareness and Training

• The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.
• Information security awareness training shall be included in the staff induction process and shall be carried out annually for all staff
• An on-going awareness programme shall be established and maintained in order to ensure that staff awareness of information security is maintained and updated as necessary.

Intellectual Property Rights

• The organisation shall ensure that all software is properly licensed and approved by the Manager / administrator. Individual and FH intellectual property rights shall be protected at all times.
• Users breaching this requirement may be subject to disciplinary action.

Access management

Physical Access

• Only authorised people who have a valid and approved business need shall be given access to areas containing information systems or stored data.

Identity and passwords

• Passwords must offer an adequate level of security to protect systems and data
• All passwords shall be eight characters or longer and contain at least two of the following: upper case letters, lower-case letters and numbers
• All administrator-level passwords shall follow NCSC guidelines (see https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach)

• Where available, two-factor authentication shall be used to provide additional security
• All users shall use uniquely named user accounts
• Generic user accounts that are used by more than one person or service shall not be used

User Access
• Access to information shall be based on the principle of "least privilege" and restricted to authorised users who have a need to access the information.

Administrator-level access
• Administrator-level access shall only be provided to individuals with a business need who have been authorised by the FH Manager.
• A list of individuals with administrator-level access shall be held by the FH Manager and shall be reviewed every 6 months
• Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.

Application Access
• Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.
• Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access
• Where indicated by a risk assessment, access to the network shall be restricted to authorised devices only

System Perimeter access (firewalls)
• The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.
• All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.
• The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed regularly
• All firewalls shall be configured to block all incoming connections.

• If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.

Monitoring System Access and Use

• An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.
• The Centre reserves the right to monitor and systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

Asset Management

Asset Ownership
• Each information asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Asset Records and Management

• An accurate record of FH information assets, including source, ownership, modification and disposal shall be maintained.
• All data shall be securely wiped from all hardware before disposal.

Asset Handling

• FH shall identify particularly valuable or sensitive information assets through the use of data classification.
• All staff are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.
• All organisation information shall be categorised according to the risk assessment and shall be handled according to the risk appetite defined in that policy.

Removable media

• Only FH approved removable media (such as USB memory sticks) shall be used to store FH data it will be encrypted and its use shall be recorded.
• Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of FH's Manager before they may be used on business systems. Such media must be scanned by anti-virus before being used.
• Where indicated by the risk assessment, systems shall be prevented from using removable media.

Users breaching these requirements may be subject to disciplinary action.

Mobile working

• Where necessary, staff may use organisation-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements

• Use of personal mobile devices for business purposes (whether business-owned or personal devices) requires the approval of FH's Manager.

• Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.

• Users must inform FH's Manager immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

Personal devices / Bring Your Own Device (BYOD)

• Where necessary, staff may use personal End User Devices (EUDs), i.e., mobile phones, laptops, tablets etc., to access email. Content may only be stored on encrypted devices approved by the Manager. The device must be recorded in the asset register and must be configured to comply with the mobile working section and other relevant sections of this policy.

• No other personal devices are to be used to access business information

Social Media

• Social media may only be used for business purposes by using official business social media accounts with authorisation. Users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.

• Access to all FH business facilities and functions will be restricted to duly identified and authenticated authorised individuals.

• Social media accounts used by the FH shall be protected by strong passwords in-line with the password requirements for administrator accounts.

• Users shall behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent centre. If in doubt, consult FH's Manager.

• Users breaching this requirement may be subject to disciplinary action.

Physical and Environmental Management

• In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Physical security accreditation should be applied if necessary.
• Systems shall be protected from power loss by UPS if indicated by the risk assessment.
• Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

Computer and Network Management

Operations Management
• Management of computers and networks shall be controlled through standard documented procedures that have been authorised by FH's Manager .

System Change Control

• Changes to information systems, applications or networks shall be reviewed and approved by FH's Manager .

Accreditation

• FH shall ensure that all new and modified information systems, applications and networks include security provisions.
• They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved.

Software Management

• All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.
• All software security updates/patches shall be installed within 7 days of their release.
• Only software which has a valid business reason for its use shall be installed on devices used for business purposes
• Users shall not install software or other active code on the devices containing business information without permission from [title].
• For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes.

Local Data Storage

• Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals (at least monthly).
• A backup copy shall be held in a different physical location to the business premises

• Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

Data Protection

• Data in transit will always be protected by encryption (TLS or IPsec)
• Data at rest will be protected as follows:

- Personal data will be encrypted, (this is in line with GDPR requirements) and keys held by trusted custodians.
- Other sensitive information, i.e., information where the confidentiality impact is assessed at medium or above, will be encrypted and keys held by trusted custodians.
- All other data will be protected by restricting access to identified and authenticated authorised individuals.

External Cloud Services

• Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider') there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

Protection from Malicious Software

• The business shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.
• All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system
• All anti-malware software shall be set to:

- scan files on-access
- automatically check for, daily, virus definitions and updates to the software itself and install new versions when they become available
- block access to malicious websites

Vulnerability scanning

• The business shall have a regular vulnerability scan of all external IP addresses carried out by a suitable external organisation
• The business shall act on the recommendations of the external organisation following the vulnerability scan in order to reduce the security risk presented by any significant vulnerabilities

• The results of the scan and any changes made shall be reflected in the organisation risk assessment and security policy as appropriate.

Information security incidents

• All breaches of this policy and all other information security incidents shall be reported to the Centre Manager.

• All other information security incidents shall follow a SIR (Security Incident Response) procedures which require:

- If required as a result of an incident, data will be isolated to facilitate forensic examination.
- Information security incidents shall be recorded in the Security Incident Log
- The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.

• Identify and assign information security roles and responsibilities appropriate to the size, structure and business function of their organisation;

• Adopt policies, procedures and controls to ensure information assets are identified, valued, handled, stored, processed, transmitted, shared and destroyed in accordance with legal requirements;

• Manage the risks associated with digital continuity and records management in respect of all data held electronically, particularly in the event of upgrades in technology, transferral of data into archives and the overall life cycle of data;

• Assess any security and business risks before deciding to outsource or offshore information and/or services. Data or services that relate to or directly support national security should not normally be off shored.

Privacy Statements

FordHaven must provide a privacy statement to all data subjects, for which we hold data. This should be in line with ICO guidance about following GDPR. Procedures must be in place covering the receipt, storage, correction and deletion of personal, including special category, data.

Valuing and Classification Assets

FordHaven must ensure that information assets are valued, handled, shared and protected in line with the standards and procedures set out in legal obligations and undertakings

To comply with this requirement FH will ensure that:

• Information and other assets are valued according to the definitions the classification policy and are clearly and conspicuously marked. Where this is impractical (e.g. a building or physical asset) staff must be made aware of the protective controls required;

• Assets are protected in line with the risk appetite and countermeasures, defined in the risk assessment, throughout their life-cycle from creation to destruction to ensure a proportionate level of protection against the real and/or anticipated threats faced by such assets;
• Access to sensitive assets is only granted on the basis of a genuine need to know and an appropriate level of personnel security control;
• Where information is shared for business purposes the FH must ensure the receiving party understands the obligations and protects the assets appropriately;

Risk Assessment and Accreditation of ICT Systems

Business Continuity and Disaster Recovery Plans
• The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.
• The following arrangement shall be followed:

Risk	**Likelihood Score**	**Mitigation Plan**
Loss of staff: As a contact centre many skill sets are very critical to the organisation.	B. High Impact, Low Likelihood.	Capture as much information as possible. Prioritise having staff and volunteers that provide redundancy.
Loss of premises: e.g. building burns down.	B. High Impact. Low Likelihood.	
Loss of key supplier:	D. Low Impact. Low Likelihood.	Contractual arrangement shall be put into place which supports the transfer of services to alternative suppliers if required.

Approved by: Roxana Ford - Director
Last reviewed: March 2024
Next review due by: March 2025