ELDONIAN

ELDONIAN	ICT & Digital Policy Manual
	Doc No: 14

Version No	Title	Author	Draft Date	Approved By	Approval Date	Live Date	Review Date
1	Information Security and Infrastructure Plan	P Latham	Oct 24	Board	Oct 24	Oct 24	Oct 27
1	ICT Business Continuity and Resilience Policy	P Latham	Aug 24	Board	Aug 24	Aug 24	Aug 24
1	ICT & Digital Policy Manual	P Latham	Oct 24	Board	Oct 24	Oct 24	Aug 24

ICT Business Continuity & Resilience Policy

1. Introduction

This policy seeks to outline the organisations approach to keeping its ICT resources secure and resilient and outline its approach to ICT business continuity in the event of a cyber-attack.

2. ICT Security

The ECBHA approach to ICT security is informed by the International Standard ISO 27001. The Code of Practice for Information Security Management, which is the de facto standard for the development of information security strategy world-wide.

We have an obligation to clearly define requirements for the use of our ICT facilities and systems so that users do not unintentionally place themselves, or the organisation at risk.

Information and data play a major role in supporting organisations strategic and administrative activities and we must adequately protect it from internal and external security threats, whether deliberate or accidental.

ICT security controls are designed to protect:

- Confidentiality - knowing that key data and information can be accessed only by those authorised to do so.
- Integrity - knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,
- Availability - knowing that the key data and information can always be accessed.

Our security approach applies to all '*subjects*', defined as all full-time, part-time and temporary staff employed by, or working for or on behalf of ECBHA either in paid or voluntary positions,

contractors and consultants and all other individuals granted access to The Group's ICT systems, data and information.

The Board is ultimately responsible for ensuring ICT security, operationally this responsibility is delegated to the Chief Operating Officer (COO). It is the personal responsibility of each subject to adhere with this document's requirements.

2.1 ICT Security - Information Security Infrastructure Plan (ISIP)

An ISIP will be developed in conjunction with ECBHA's ICT related contractors and service providers. This will include:

- A summary overview of all ICT security precautions including the controls deployed to reduce the risk of human error, theft, fraud, nuisance or malicious misuse of information and facilities.
- An expectation of how ECBHA contractors and service providers will ensure security precautions remain adequate.
- Agreed authorisation processes regarding facilitating third party access to ICT provisions and systems.
- Agreed approach to managing risk from authorised and unauthorised third part access including remote and home working.
- Agreed arrangements and assurance for passwords control, storage and back up arrangements.

The ISIP will be reviewed annually and will form part of the wider service level agreement with contractors and service providers as appropriate.

2.2 ICT Security – Controls Register

All data and information assets held will be identified, categorised and recorded in a suitable control register to enable appropriate management and control and security. This control register will also include an inventory of hardware and software.

As with the ISIP, this ICT control register will be reviewed at least annually to ensure precautions remain appropriate.

2.3 ICT Security – ECBHA Staffing

When reviewing job descriptions ECBHA will seek to define ICT security related responsibilities and access. When recruiting ECBHA will be mindful of ICT security risk when considering the background of candidates in a fair manner.

All members of staff are reminded of their obligation to protect confidential information in accordance with The Group's standard terms and conditions of employment.

Employees will be informed of their information security responsibilities during induction training, and this will be reiterated on an ongoing basis. Information security awareness training and / or instruction will be made available to staff.

Staff and other subjects are responsible for safeguarding key data by ensuring that desktop machines are not left logged-on when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.

Where available, password protected screensavers and automatic log-out mechanisms are to be used on office-based systems to prevent individual accounts being used by persons other than the account holders.

2.4 ICT Security - Responding to Security Incidents

Subjects must not try and prove any suspected or perceived security weakness. All actual and suspected security weaknesses and incidents are to be reported to the COO and the appropriate ICT contractor (usually Abyss or SDM) immediately.

Any computer that is perceived to be placing the integrity of the network at risk will be disconnected at the network boundary. Subsequent reinstatement will only be permitted once the integrity of the system has been verified

Events that are regarded as being 'security incidents' will be defined, and a process agreed between ECBHA and its ICT contractors to investigate, control, manage and review such events with a view to preventing recurrence.

2.5 ICT Security – Operational Management.

Controls will be implemented to enable the correct and secure operation of information systems, information and data processing through the ongoing development of organisational procedures that are mindful to ICT security. Where appropriate ICT contractors and service providers will be included in the development of operational procedures.

Sensitive documentation will be held securely, and access restricted to staff on a need-to-know basis. An agreed overview of access will be reviewed annually as part of the ICT Security control register.

Access to critical systems and key data and information will only be granted on a need-to-know basis with permanent and full access to live operating environments being restricted on role-based requirements.

Particularly sensitive information and data relating to highly confidential matters and projects will be identified and specific secure storage arrangements agreed by the Chief Executive Officer with ECBHA contractors and service providers as appropriate.

Appropriate capacity planning will be undertaken and reviewed annually, alongside agreeing protocols alerting capacity issues within critical systems.

Controls within the ISIP will be implemented to check for malicious or fraudulent code being introduced to critical systems, ensure appropriate anti-virus precautions and virus containment arrangements.

Archiving reviews will be undertaken annually in accordance with the National Housing Federation guidance regarding data retention.

Any data holding media, for example memory sticks, will only be used as a last resort and with the authorisation of the COO. Such devices will be logged and managed within the ICT security control register.

Redundant computer equipment will be disposed of in accordance with the Waste Electrical and Electronic (WEEE) Regulations and through secure and auditable means.

Information and data should only be shared via electronic means. No third-party media, for example memory sticks, must be used to import information or data. If such an action is unavoidable, this should be approved by the COO and with guidance / monitoring of the appropriate ECBHA contractor / service provider.

Software will be used, managed and controlled in accordance with legislative requirements. All major software upgrades for critical systems will be undertaken by experienced appropriate ECBHA contractors / service providers who will outline to ECBHA the appropriate controls and testing they will undertake to deliver live implementation.

Access to and use of critical systems will be monitored using various software technologies and reports will be provided to ECBHA by its contractors / service providers upon request.

Test and development systems will be appropriately isolated from live critical systems at all times.

2.6 ICT Security - Security Responsibilities

The COO is responsible for:

- Monitoring and managing ICT security compliance and receiving / reporting suitable assurances and testing by ECBHA third party contractors and service providers.
- Ensuring cost effective services by ECBHA third party contractors and service providers.
- Delegating technical security responsibilities to staff within ECBHA third party contractors and service providers.
- Communicating ICT security requirements to staff, and other authorised users ensuring they are aware of their personal security responsibilities.
- Ensuring the ISIP and ICT Control register are in place, updated at least annually and provide confirmation of such to the Board.
- Ensuring that ICT security risk is appropriately represented in the organisations wider risk management.
- Acting as the focal point for information security issues within ECBHA, for both staff and external organisations.
- Receiving and disseminating information regarding ICT security incidents and responses.

3 Acceptable Use

The following are defined as acceptable / not acceptable use of the ECBHA ICT provisions and systems:

3.1 Email

Acceptable use

- Work-related use in line with business requirements and business etiquette, however before using email it should be considered if there are other business systems that

would be more appropriate for recording or communicating the intended information /data. This can include communications with colleagues, customers, third party organisations and other business-related parties.
- Use in relation to professional development, networking, education and training and wider engagement with the organisations sector and locality.
- Limited personal use in urgent / emergency situations and to provide appropriate wellbeing support/contact to colleagues.
- Subscribing to business requirements related newsletters and subscriptions.
- Sending and receiving attachments and secure data links related to any of the above.

Unacceptable Use

- General personal use.
- Anti-social or unacceptable usage, for example passing on chain mail, jokes, inappropriate links to websites, spam, animations, hoax virus warnings etc.
- Operating third party businesses or undertaking business activities on behalf of other employers or clients.

3.2 Internet access/ECBHA WIFI:

Acceptable Use

- Accessing, downloading and uploading work-related resources, information, reports and accessing web-based services in line with business requirements and business etiquette.
- Personal web browsing during lunch and other breaks provided the content would be deemed appropriate viewing for all colleagues within the workplace.
- Personal devices can be connected to the Wi-Fi based on these accepted uses and that the upload/download rate for the device is not negatively impacting on ECBHA devices.

Unacceptable Use

- Accessing anything that would be considered illegal, immoral or would be likely to offend colleagues in the workplace.
- Operating third party businesses or undertaking business activities on behalf of other employers or clients.
- Downloading or uploading files of such significant size that they are likely to impact on the connectivity for other users.
- Saving usernames and password to personal accounts and subscriptions within the ECBHA provided browser.
- Personal device being connected to the Wi-Fi that negatively impact the performance of ECBHA devices or that pose an ICT security risk.

3.3 Shared drives and folders

Acceptable Use

- Saving work-related content in line with business requirements and business etiquette, however before saving to a shared drive or folder it should be considered if there are other business systems that would be more appropriate for storing the intended information /data. Wherever possible all personal data relating to customers must be stored within appropriate fields within SDM.

Unacceptable Use

- All personal use.
- Saving documents for unrelated third-party business activities or business activities on behalf of other employers or clients.

3.4 Personal drives and folders

Acceptable Use

- Saving work-related content in line with business requirements and business etiquette, however before saving to a shared drive or folder it should be considered if there are other business systems that would be more appropriate for storing the intended information /data.
- Personal documents relating to employment, professional development, networking, education and training and wider engagement with the organisations sector and locality.
- Other occasional personal documents, however, subjects should remain aware that personal drives provided by ECBHA can be accessed and/or deleted by the organisation without notice.

Unacceptable Use

- Excessive / inappropriate personal use.
- Saving anything that would be considered illegal, immoral or would be likely to offend colleagues in the workplace.
- Saving documents for unrelated third-party business activities or business activities on behalf of other employers or clients.

3.5 Hardware (desktops, laptops, company mobile phones)

Acceptable Use

- Work-related use in line with business requirements and business etiquette, this can include communications with colleagues, customers, third party organisations and other business-related parties.
- Use in relation to professional development, networking, education and training and wider engagement with the organisations sector and locality.
- Limited personal use in urgent / emergency situations and to provide appropriate wellbeing support/contact to colleagues.

- For portable devices, use in locations that are appropriate and safe for both the subject and the device and in conjunction with appropriate bags / covers to protect the wellbeing of the subject and to protect the device.

Unacceptable Use

- Excessive / inappropriate personal use.
- Accessing or saving anything that would be considered illegal, immoral or would be likely to offend colleagues in the workplace.
- Undertaking work or accessing resources for unrelated third-party business activities.
- For portable devices, use in locations that are inappropriate and put the wellbeing of the subject at risk and/or doesn't adequately protect the device.
- For portable devices, allowing any unauthorised third-party individuals, for example family or friends, to use the equipment for any purpose.
- Connection of any removable storage media, for example memory stick for the access, upload or download of information or data without authorisation

4 Cyber Incident Response

This content describes our approach for malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out.

Every incident is different, and the steps taken at each stage may vary in relevance or severity given the nature and impact of the incident. Dealing with an incident is not a linear process and activities in each area may be initiated synchronously, revisited for in-depth action after a quick pass through and completed at different times.

Incident response can be initiated by several types of events, including but not limited to:

- Automated detection systems or sensor alerts
- Contractor or third-party ICT service provider report / detection of network activity to known compromised infrastructure, detection of malicious code, loss of services, etc
- Analytics that identify potentially malicious or otherwise unauthorized activity
- Internal organisational situational awareness

It is most likely that any technical detection or alert will come through one of ECBHA ICT service providers. However, if an incident bypasses the safeguards put in place, then ECBHA may become directly aware due to impact on the systems and software.

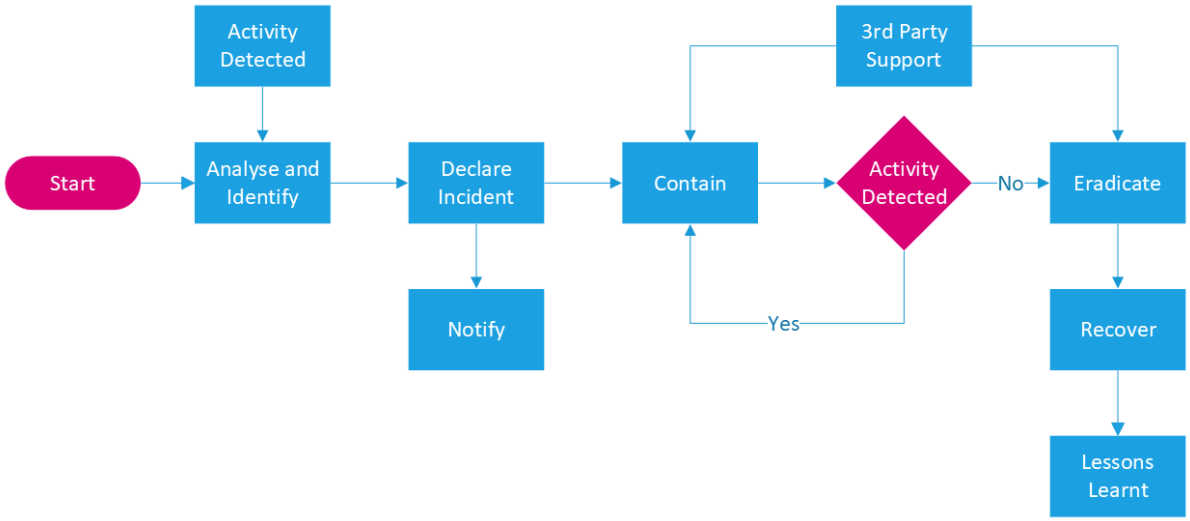
This approach is intended for incidents that involve confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out, for example:

- Incidents involving lateral movement, credential access, exfiltration of data
- Network intrusions involving more than one user or system
- Compromised administrator accounts
- Ransomware

It does not apply to activity that does not appear to have such major incident potential, such as:

- Classified information incidents that are believed to result from unintentional behaviour only
- Users clicking on phishing emails when no compromise results
- Commodity malware on a single machine or lost hardware

4.1 Cyber Incident Response - Incident Response Flow Chart



As previously stated, the detection of a suspicious cyber activity is most likely to occur through an ECBHA ICT service provider but there remains the possibility that it could be detected directly by the association. Therefore, at point of detection, ICT service providers will notify ECBHA and vice versa.

4.2 Cyber Incident Response - Analyse and Identify

The initial priority is to understand enough to declare an incident and take containment and mitigation actions quickly. Declaring an incident should not be delayed.

This will be undertaken by the relevant ECBHA ICT service provider.

Key information to know

- Nature of incident
- Scope
- Is it active
- Collation of initial indications, for example IOCs, attack vectors, IP ranges, intelligence from firewall tools

Key questions to answer

- What was the initial attack vector?

- How did the adversary gain initial access to the network?
- How is the adversary accessing the environment?
- Is the adversary exploiting vulnerabilities to achieve access or privilege?
- How is the adversary maintaining command and control?
- Does the actor have persistence on the network or device?
- What is the method of persistence?
- What accounts have been compromised and what privilege level?
- What method is being used for reconnaissance?
- Is lateral movement suspected or known?
- How is any identified lateral movement conducted?
- Has data been exfiltrated and, if so, what kind and via what mechanism?

4.3 Cyber Incident Response - Declare Incident

The ICT service provider and a representative of the ECBHA Leadership Team will communicate by a method that is believed to secure, most likely phone, and discuss the analysis and identification outcomes. A decision will be clearly made if, or if not, the suspicious cyber activity will be declared as a cyber incident. If an incident is declared:

- The ICT service provider will define the technical steps necessary to respond to contain the incident.
- ECBHA will define the steps it needs to take ensure that staff and customers are safeguarded and decide if the ECBHA critical incident plan needs to be invoked.
- Depending on the incident a communications protocol will be agreed that ensures communications are not impacted by the incident.

4.4 Cyber Incident Response – Notify

ECBHA Chair and Leadership Team will be notified of the incident and any involvement they need in proposed actions.

ECBHA will notify any relevant third parties, these could include the Police, Information Commissioners Office (ICO), and Regulator of Social Housing (RSH) dependent on the nature of the incident and if a critical incident response has been invoked.

4.5 Cyber Incident Response – Contain / Mitigate

The ICT service provider will seek to implement short-term mitigations to isolate threat actor activity and prevent additional damage from the activity or pivoting into other systems. This stage maybe initiated before the Notify stage, certainly in a measured way to affected areas of the infrastructure as soon as malfeasant activity is detected to isolate the attack and minimise wider impact.

Appropriate containment activities need to be based on the perceived threat at the time and current knowledge of the nature of the incident along with the anticipated impact. Some attacks may not need a full internal containment process however, until that is known for it is actions will be based on address the worst-case scenario.

4.6 Cyber Incident Response – Remediate / Eradicate

The aim of this stage is to fully remove the threat from the network and systems. This often involves similar actions to containment but is sometimes coordinated so that all actions are carried out simultaneously.

It is important to confirm that remediation has been successful before moving to the recover stage - this may involve monitoring for a period. Some analysis may continue in this stage too.

- Determine nature of compromise
- Determine date of compromise and last known clean backup date
- Validate virus and vulnerability scanning software will detect infection(s)
- Confirm residual artefacts and secondary infections are not present
- Evidence of data exfiltration
- Preserve logs and other evidence for 3rd party investigation
- Respond to appropriate external representative's requests
- Integrity of infrastructure / confirm free from infection

4.7 Cyber Incident Response – Recover

At this point, systems are returned to 'business as usual'. Clean systems and data are put back online, and in some cases, final actions are taken to handle regulatory, legal, or PR issues.

- Segregate "known clean" materials from any "unknown" or "known dirty" materials
- Form themed recovery teams to develop and enact the solutions to each area of the infrastructure that needs recovered

4.8 Cyber Incident Response – Golden Rule

Nothing gets connected to the network until it is verified as clean and signed off with peer review.

5 Review

This policy will be reviewed at least every three years and represented to Board for approval.

ECBHA will engage its ICT provider to ensure that suitable provisions are in place to enable ECBHA owned or leased mobile devices to be remotely managed (mobile device management) and the applications installed on these devices (mobile application management). This will include:

- Ensuring all devices are suitably enrolled and managed within the organisation information infrastructure and security precautions.
- The ability to remotely restrict or disable mobile devices where a function or user is deemed to present an unacceptable potential security risk.
- Ability to wipe organisational data from the device.
- Enforce password/pin policies
- Ensure devices are running a suitably supported version of the operating system

ECBHA Information Security Infrastructure Plan (ISIP)

1. **ISIP Purpose**

The ISIP seeks to define:

- The precautions that ECBHA will undertake to support the information security of its ICT related infrastructure.
- A network security plan is a strategy that defines the approach and techniques used to protect the network from unauthorized users and guards against events that can jeopardize or compromise a system's security.

The approach and techniques used by an organization may consist of creating security policies and procedures that describe how an organization intends to meet the security requirements for its systems.

2. **Business Model Summary**

ECBHA is a small housing provider offering a limited range of housing products.

The main ECBHA function is that of a social landlord, renting the homes that it owns to the public on a long term basis. It also provides:

- A small number of shared ownership properties
- Leasehold management to one private development.
- A care home leased in full to an independent operator.
- A village hall leased in full to an independent operator.

ECBHA is:

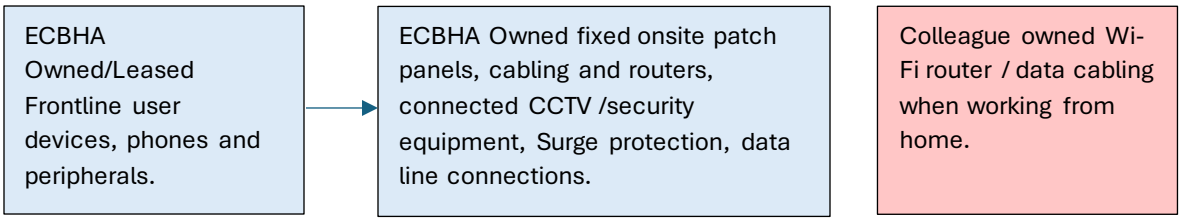
- In contact with its residents principally in person, by phone and by email and has recently launched a resident self service portal.
- Open to the public standard office hours Monday to Friday but also offers a phone based emergency only service outside these hours.
- Has a Board agreed very low appetite for risk.
- Reliant on eternal providers for its ICT provisions and support as it does not have an economy of scale to support in-house resources.

The information held by ECBHA can be summarised as:

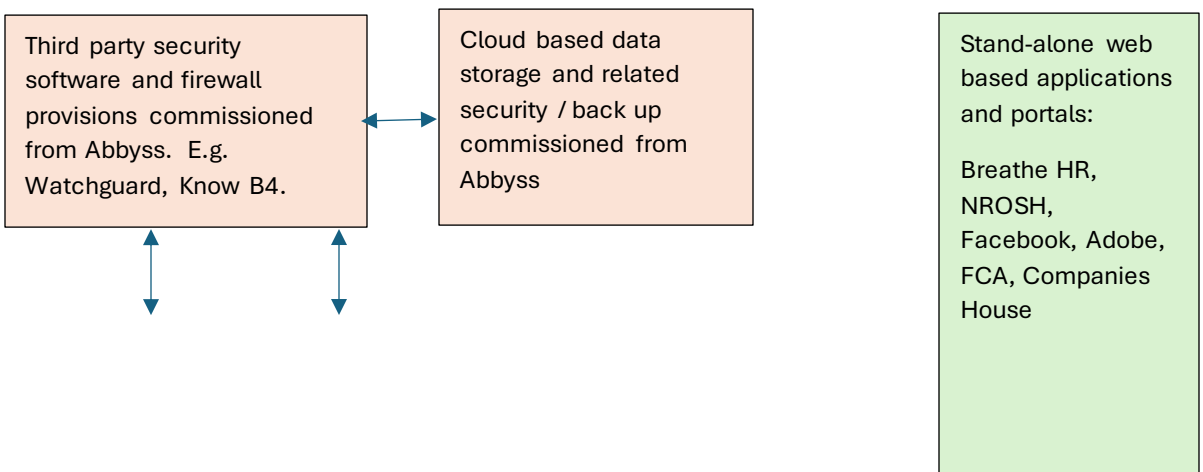
- Personal information regarding applicants and tenants.
- Operational information regarding the delivery of our services.
- Technical information regarding the homes we provide.
- Organisational information regarding our business including financial, governance, strategic and regulatory information.
- Personal information regarding ECBHA colleagues and Board members.
- Information provided by partner organisations.

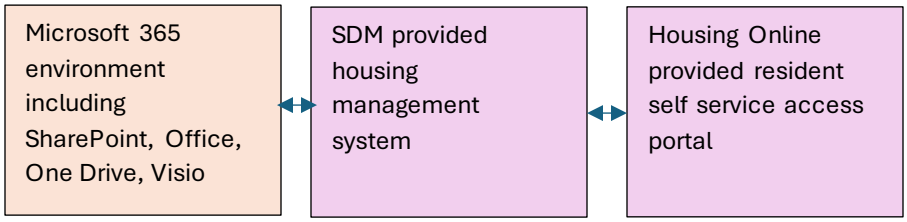
3. ECBHA Information Infrastructure Map

A. Hardware.



B. Software.





	ECBHA owned or leased mobile or fixed equipment maintained by Abbyss
	Standalone colleague owned/maintained connectivity hardware when home working
	Third party provisions commissioned by Abbyss of ECBHA behalf
	Third party provisions commissioned by ECBHA directly
	Standalone applications accessed only via we browser

4. ECBHA ISIP Elements

Based on the business model the ISIP comprises the following precautions:

4.1 Policy.

Having in place a current ICT Business Continuity & Resilience Policy reviewed on at least a three yearly basis and more often should new information security threats emerge, existing threats evolve or the business model change. This will also outline the approach to responding to incidents.

4.2 Assessment.

Undertake an assessment, in conjunction with ICT providers, of ICT infrastructure threats annually and ensure that any identified threats are suitably mitigated and reported by Leadership to Board to inform the wider risk management framework.

4.3 Testing.

At least annually, the ICT provider will undertake vulnerability scan testing of the organisations infrastructure environment. This is anticipated to include firewalls, network segmentation, endpoint malware protection, security awareness programs, overall encryption, testing effectiveness to varying threat types. The outcomes will be confirmed to ECBHA and recommendations made for mitigations and/or the need for detailed penetration testing.

4.4 Culture.

The actions of end users provides the biggest information security threat. Leadership will seek to instil a culture of ‘security first’ through both individual and collective staff management. This will be supported by inductions for new starters,

regular training/reiteration of security requirements and checks of compliance with required operational practices.

Leadership will receive regular ICT security training completion reports from the provider and non-compliance will be progressed with individual members of staff.

4.5 Hardware.

Day to day, only ECBHA owned devices, with up to date security software and password protection, will be used to access and use information held by ECBHA. Personal devices must not be used as part of the ECBHA infrastructure / environment. The only exception being colleagues home wifi routers which may be used is suitable secure as outlined in section 4.11.

The number of devices will be minimised as much as operationally possible and all other options will be considered before additional hardware.

All hardware to be audited annually. A record of hardware being issued and returned will be held by the Company Secretary.

Policy statements will be in place regarding mobile device management and a recognised mobile devise management system will be agreed and put in place.

USB ports will usually be disabled on all ECBHA devices unless an individual has a specific need that is approved and recorded in the control register. Only ECBHA owned USB memory devices must be used on any hardware within the organisations infrastructure which will be equipped with appropriate protection by the ICT provider.

'Smart' web enabled devices and appliances continue to grow in popularity. Such devices used within ECBHA must come through reputable supplier and manufacturers. The ICT provider must be consulted to ensure that any risk is quantified and managed prior to connection. These will be logged in the hardware register.

Redundant hardware will be disposed of by the ICT Provider in a secure manner compliant with the Waste Electrical and Electronic Regulations.

4.6 Software.

All software that it proposed to be added to in the infrastructure must be demonstrated to be from a reputable source and be provided with appropriate certifications. Software will only be updated or added to the infrastructure by the trained, designated and authorised personnel of the ICT provider.

If an item of software is found to defective and pose a cyber security risk the ICT provider will isolate/remove as appropriate inline with the agreed incident response provisions.

4.7 Access & Control.

The access levels within the infrastructure for each user will be held in a controls register and checked at least annually to ensure that they remain appropriate to the user.

Arranging a new access to the ECBHA infrastructure can only be authorised by the Chief Executive Officer or Company Secretary.

Passwords are required to have at least 12 characters and multi factor authentication will be used for the access to the infrastructure.

4.8 Sharing / Transfer.

Data sharing protocols will be put in place when data needs to be transferred to a third party organisations to deliver a service on behalf. The security of the method of data transfer will be considered and risk assessed as part of agreeing these protocols. A register of data sharing protocols will be held by the Company Secretary.

4.9 Storage.

All electronic data held by ECBHA will be held off premise in a secure and backed up cloud storage provision. Staff will be supported to not store data on hardware. The security specification for the cloud storage provision will be reviewed by ECBHA and the ICT provider at least annually in line with identified and proportional best practice.

ECBHA will only hold information in hard copy where there is a legal duty or absolute operational necessity to do so. Security of hard copies will be proportionate to the sensitivity as instructed by the Company Secretary.

4.10 Simplicity.

It is easier to keep a simple system secure than one that is more complex. ECBHA will seek to ensure that it minimises the systems and software it uses from different providers to minimise the security risk of transferring information within the overall infrastructure.

A clear business and risk assessment needs to be approved by the Chief Executive Officer for any proposed new business systems or software.

4.11 Connectivity.

In ECBHA premises, hardware must be connected to the wider organisational infastructure via hard wired ports, if available or the organisation password protected wifi.

All staff will be regularly reminded how to identify the correct wifi connection to minimise the risk of imposter connections being used to harvest user names and passwords.

When out of the office, all hardware, when used should connect via the data service available through the ECBHA provided mobile phone. Public and free wifi services should be avoided unless absolutely necessary as their security risks are unknown.

When home working, colleagues need to ensure that they have in place adequate precautions to ensure that their home data / wifi provision is sufficiently secure. The ICT Provider will perodically provide training and updates regarding the precautions that need to be in place to ensure that these home based connections are secure. If a colleague is not confident that that their home connect has the recommended security in place then they should connect via the ECBHA mobile phone data connection or work from the office.

4.12 Insurance.

While this plan seeks to largely take preventative action it is impossible to safeguard against all potential scenarios. Therefore ECBHA will hold cyber security insurance to mitigate should an attach occur. The requirements of the insurer to ensure that cover is maintained is expected to add further precautions to the plan.

5. Accreditations and Assurance

ECBHA expects its ICT providers to be able to demonstrate compliance with the following recognised standards:

- ISO27001 Certification.
- IASME GOLD.
- Cyber Essentials Plus.
- ISO 4001 Certification.
- ISO 9001 Certification.

ICT providers are also required to hold professional liability insurance for £5,000,000 and cyber liability insurance for £500,000.

In addition ECBHA will seek further assurance of its information security precautions through a cyber security audit at least every three years.

Where significant cyber attacks and 'near misses' are identified, or incidents do occur, the ICT provider and ECBHA will meet to identify and any lessons learned and actions to be undertaken.

Annually the management will confirm to the Board that these ISIP precautions remain place and have been reviewed, in conjunction with the ICT provider. This will be reported based on the format outlined in Appendix 1.

6. **Future Development**

This plan is a living document, that requires review at least annually to ensure it is current and up to date with regulatory requirements or major changes to the business and its required information infrastructure.

ECBHA does not currently hold Cyber Essentials or Cyber Essentials Plus accreditation, however this is held by the current ICT services provider. In due course as the ECBHA information security mature ECBHA will consider seeking a direct accreditation against these standards.

Appendix 1:

ISIP Annual Review Format

Introduction
Date of Review:
Carried out by:
ECBHA:
ICT Provider(s):

ISIP Precautions Review			
Review Item	**In Place**	**Up to Date**	**Notes / Actions**
	Yes/No	Yes/No	
ISIP related policies			
Incident response in place			
Incident response plan awareness			

ELDONIAN

Annual threats assessment			
Vulnerability scan			
Information security inductions			
Information security training			
Hardware register			
Access register			
Control register			
Data sharing register			
Hardware audit			
Compliant hardware disposals			
Passwords compliance			
Cloud storage specification review			
Working from home precautions			
Insurance			

Incidents Review
Summary of Incidents and Identified 'Near Miss':
Identified Learning:
Actions Undertaken:
Actions to be Taken:

Conclusion
Position Summary:
Actions / Recommendations Summary: