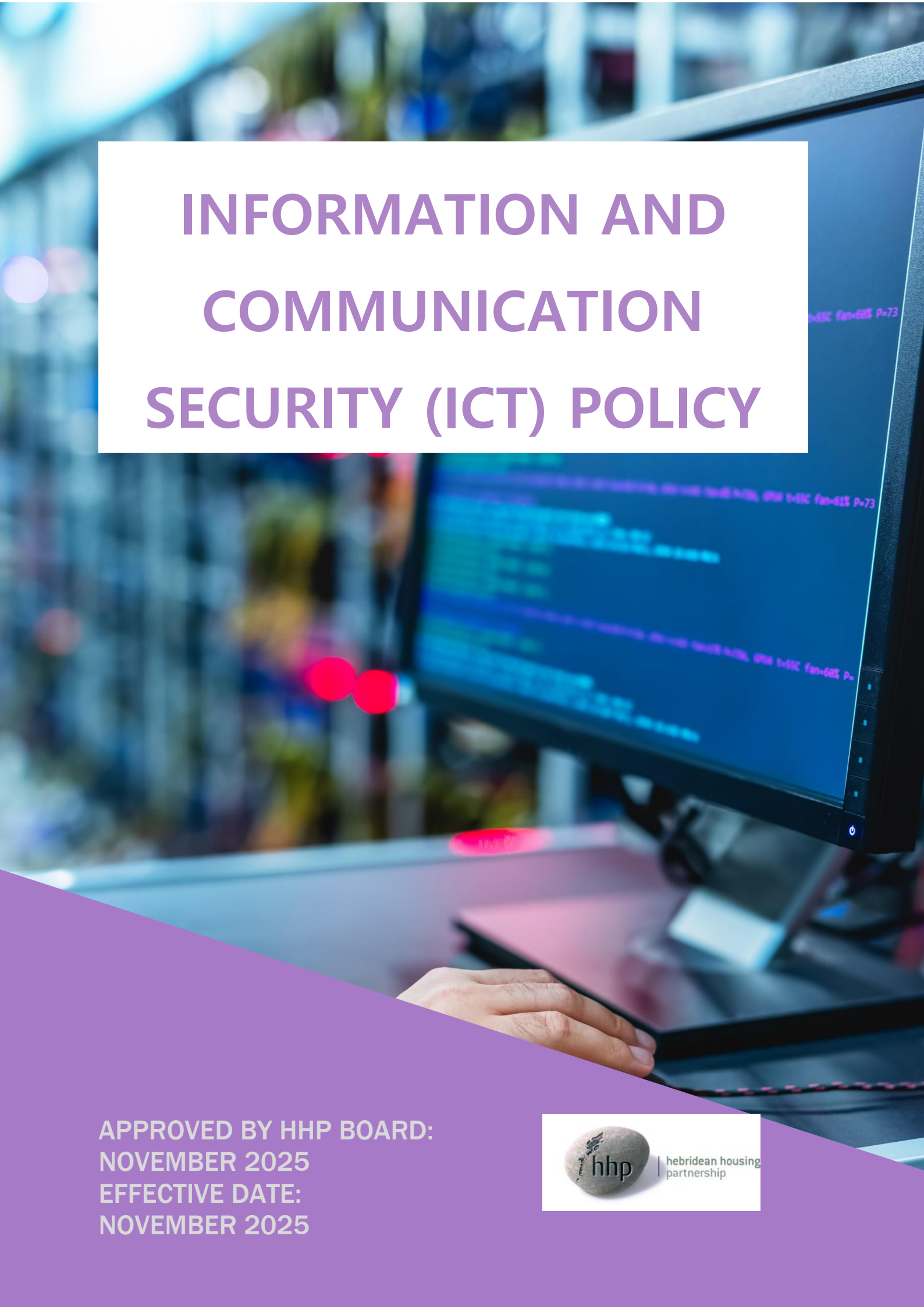

INFORMATION AND COMMUNICATION SECURITY (ICT) POLICY

APPROVED BY HHP BOARD:
NOVEMBER 2025
EFFECTIVE DATE:
NOVEMBER 2025

hhp | hebridean housing partnership

TABLE OF CONTENTS

INTRODUCTION

1.1 The purpose of the ICT Security Policy is to protect the organisation's information assets and ICT systems from all threats—internal or external, deliberate or accidental.

1.2 This policy applies to all Board Members, employees (including temporary staff and students) and organisations acting on our behalf. It applies to all locations where information and data are accessed and used.

1.3 This Policy applies to all IT-related systems, hardware, services, facilities, and processes owned or otherwise made available by Hebridean Housing Partnership (HHP) or on its behalf, whether utilising HHP's network and servers or those provided through cloud-based environments.

1.4 This will be achieved through the:

a) Management of security risks;
b) Protections against information loss and cyber-attack;
c) Detection of information loss and cyber security events; and
d) Minimisation of the impact of these security incidents.

ICT SECURITY RISKS

2.1 Housing associations face growing and increasingly sophisticated security threats. These include risks such as:

- ICT systems and networks are vulnerable to fraud, data theft, surveillance, and vandalism.
- Greater reliance on IT services and the expansion of networking, cloud services, and mobile devices creates more entry points for unauthorised access and reduces central control.
- Integration and data sharing—along with emerging technologies like AI and machine learning—introduce new security challenges.

MANAGING SECURITY RISKS

GOVERNANCE

3.1 We are committed to achieving the highest standards in protecting the information, and to embody the following three objectives in our approach to information security:

a) Confidentiality — Only individuals with authorisation can or should access data and information assets.

b) Integrity — Data should be intact, accurate and complete, and IT systems must be kept operational.

c) Availability — Users should be able to access information or systems when needed.

3.2 The Director of Finance & Corporate Services will be the primary point of contact for the Board and Executive Team, supported by the Corporate Resources Manager and the Data Protection Officer.

- The Corporate Resources Manager will be responsible for the day-to-day security management and update of policies and procedures.
- The Data Protection Officer (DPO) is responsible for making sure an organisation follows data protection laws, providing guidance on privacy practices, and managing responses to data breaches and information requests.

RISK MANAGEMENT

3.3 This Risk Register will be provided together with the corporate Risk Register, which is accessible to the Board.

3.4 All announced vulnerabilities in software packages should be reviewed, tracked and mitigated.

3.5 All employees receive regular ICT security training to ensure they understand their responsibilities in protecting the organisation's digital assets. This training will cover key topics such as password management, phishing awareness, data handling procedures, and incident reporting protocols. Staff are expected to maintain a baseline level of cybersecurity knowledge appropriate to their role, and refresher

sessions will be provided periodically to address emerging threats and reinforce best practices.

3.6 Regular threat and resilience testing (both by table-top and physical exercises) will be undertaken to evaluate the viability and effectiveness of our processes, and any changes required will be merged into our Disaster Recovery and Business Continuity policies and plans.

3.7 We will ensure that our security systems are regularly audited by our internal Audit process, and by other external processes (Cyber-essentials accreditation for example).

ASSET MANAGEMENT

3.8 An up-to-date inventory is maintained of all our IT assets (hardware and software, and the location, ownership and function of each asset will be clearly stated.

3.9 Assets will be prioritised to reflect their importance in supporting and delivering essential business functions including details of other critical dependencies such as power, connectivity, cooling etc.

SUPPLY CHAIN MANAGEMENT

3.10 Appropriate vetting of 3rd party suppliers is undertaken prior to entering into any agreements.

3.11 All external suppliers who have access to HHP IT Systems or data must work under the supervision of HHP staff and in accordance with this Policy.

3.12 We will provide a copy of this policy to each third-party support provider and obtain written agreement of compliance at the commencement of any new contract or as this policy changes.

3.13 Critical data links with other organisations have their access rights regularly reviewed and systems are in place to protect data from being shared, whether in storage or during travel (firewalls, read-only/time-bound access, VPN's and encryption for example).

3.14 We will also look to ensure that software providers/suppliers have their own processes for testing for vulnerabilities within any of their products (or within 3rd part components) that have been provided to us, and that these threats are communicated to us for mutual support and resolution. If, following a review of

risks, it is decided that vulnerabilities are not being adequately managed, then we will prevent access to and use of this software until a solution is obtained.

PROTECTING AGAINST CYBER ATTACK

ASSETS

4.1 Our systems are a mixture of local PC's, tablets and servers and other equipment, based in different locations. These are integrated with infrastructure held in a remotely managed data centre or in cloud environments. Each will have its own internal and external facing control and access points that need to be secured to ensure data integrity across the organisation.

4.2 Any HHP system or equipment must kept secure at all times and be protected according to the relevant access control protocols and passkeys, using best practice wherever possible.

4.3 If you use a laptop or mobile device, you must connect to the HHP network at least every 7 days (or as soon as possible after a leave period) to pick up the latest approved patches, anti-virus definitions and security updates. Staff on long term absence should return their equipment to Corporate Resources.

FILES

4.4 All files should be saved and resaved in the latest and most secure version of that file type to ensure the file works as intended and are supported through the latest version of Software. Older files which use macros in particular will likely not be supported through the latest software given the risk of embedding malicious code within them and should be resaved in the latest format.

ACCESS, ACCOUNTS AND IDENTIFICATION

4.5 We will remove all default, shared or built in accounts on assets and software wherever possible, and where this is not possible, we will move from using the default passwords provided from the outset.

4.6 Supplier remote access accounts should remain disabled by default and enabled temporarily, as required to undertake a specific task, at the request of the system owner or administrator. Limiting access to agreed timeframes reduces the opportunity for unauthorised activities that may lead to data loss or unintended disruption.

4.7 All user rights should be reviewed when a member of staff begins employment, they change role within the organisation and critically, when they leave.

4.8 Supplier remote access accounts are made available for the remote connection to HHP's network (SecurEnvoy, or FortiClient VPN client) and must not be used to log in to servers or to run services.

4.9 User and device identification is dependent on strong and independent mechanisms, such as Biometrics or MFA – Multi Factor Authentication, being used before access to our networks and essential functions is granted.

4.10 All passkeys should meet the current organisational strength and complexity requirements as outlined in the Guidance note from Corporate Resources.

4.11 You must only access those parts of the network for which you are authorised.

4.12 You must not attempt to breach or get around our security systems or networks, for example, by probing or scanning system security, mail bombing, flooding, or broadcasting attacks.

4.13 We will run regular scans to identify unknown devices on the network.

4.14 User access logs are regularly reviewed and unusual activity investigated.

TESTING

4.15 We have ring fenced development environments for testing and development. Software is not moved into Live/Production until the relevant testing and threat analysis has been completed and signed off.

4.16 Where possible, development systems should utilise artificial or pseudonymised data and not personal data relating to individuals.

4.17 Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

BACKUPS

4.18 We will take appropriate and secured backups of all our data, both in our datacentre and in the cloud, should the original be unavailable for whatever reason.

4.19 These backups should be offline, air-gapped, and immutable as these technologies provide the strongest safeguards. These backups will be checked and periodic restores of data will be undertaken.

4.20 Safeguards are in place to protect the integrity of information during the recovery and restoration of datafiles.

4.21 Backup copies of data must be protected throughout their lifecycle from accidental or malicious alteration and destruction.

4.22 Data held on our devices should be minimised and we have the ability to remotely wipe all our mobile devices should a loss or penetration risk be identified.

4.23 Access to data backups and supporting infrastructure must be restricted to those persons who are authorised to perform systems administration or management functions.

DISPOSALS

4.24 When permanently disposing of equipment containing any storage media, all sensitive or confidential data and licensed software should be irretrievably deleted during the disposal process.

4.25 Damaged storage devices containing sensitive or confidential data will undergo assessment to determine if the device should be destroyed, repaired or discarded.

4.26 Such devices will remain the property of HHP and only be removed from site with the permission of the information asset owner. Disposal forms must be signed off by the Director of Finance and Corporate Services.

4.27 Secure disposal verification certificates should be sought for media which has contained sensitive and confidential data.

SYSTEMS DESIGN AND UPKEEP

4.28 Systems should be designed with a potential cyber incident in mind, and to support a speedy and effective means of recovery.

4.29 We will separate our networks into different security zones to allow distinctions between highly trusted and more open, internet facing parts of operation.

4.30 All systems, and especially live environments, should be patched to current or latest stable and secure versions, and should be no older than the "current minus

one version" for all other purposes. This should be done following appropriate testing and evaulation.

4.31 Any outdated computer system still in use that does not meet current security requirements, and for which there is no current alternative available, should be maintained in an offline and ring-fenced environment, with no external access possible.

4.32 Only permitted software can be installed. This list of software, on both laptops, servers and other mobile devices, will be managed by the Corporate Resources Manager. This will be reviewed regularly and added to or reduced as business needs and security issues dictate.

4.33 We will comply with all legislative GDPR data standards, including the requirement for any external cloud storage or cloud service to have its data centres within the UK wherever possible.

4.34 All our policies, processes and procedures should be designed and regularly reviewed to consider and mitigate any risks to our networks and critical systems.

4.35 Any controls implemented should however aim to provide security and defences, should our normal procedures not be followed.

EMAIL

4.36 Misuse of email or the internet is a misconduct offence and can also be a criminal offence.

4.37 Reasonable and limited personal use of email is allowed. You should be careful that a personal email is not perceived as representing HHP.

4.38 We will monitor email traffic to ensure safe and secure communication channels to and from the internet and in order to:

a) protect the organisation's systems from malicious content and spam

b) filter out hacking attempts

c) detect banned file types

d) identify any productivity issues and training requirements

e) facilitate bandwidth management and capacity planning

4.39 Users should be aware that statements made in emails can give rise to action for defamation and can lead to legally binding agreements. These can be used as evidence in legal proceedings and can also be made available on request under data protection regulations and Subject Access Requests.

4.40 Users must not transfer any of the following by email:

a) copyright photographic, audio or visual files, for example desktop wallpapers, MP3 or video files;

b) programs or applications including screensavers, animations and games;

c) files that are defamatory, offensive, obscene, abusive, threatening, contain pornographic images or covered by copyright law or any other illegal material;

d) content that constitutes harassment of another individual. This could lead to dismissal under our disciplinary procedures;

e) chain emails.

4.41 All emails will include a corporate disclaimer at its footer. This will be reviewed regularly to ensure best practice.

4.42 Users should ensure that all email communication complies with our corporate standards and best practice guidelines.

4.43 Email contact lists stored on HHP systems are the property of HHP.

4.44 If you suspect that you have received a suspicious or 'phishing' email, do not open or forward it. Report the incident to Corporate Resources. If in any doubt, delete – a legitimate email deleted in error should, in most cases be re-sent by the sender.

4.45 Ensure that links and email addresses are taking you to where you would expect to go. You can check on this by hovering over email addresses or links before use, to see if they are what they seem.

4.46 You must only subscribe to work-related mailing lists. Most viruses arrive by email and many are spread by subscriptions to mailing lists.

INTERNET ACCESS

4.47 We provide internet access for work-related research.

4.48 We will remove internet access from all systems that do not require it.

4.49 Certain sites are blocked or have limited access for system security reasons.

4.50 We allow limited personal internet browsing outside core hours for such tasks as e-banking, holiday information, flight booking, internet shopping, news and current affairs and social media. Staff must be clocked out when using the internet for personal purposes.

4.51 You must not download or transfer the following via the internet:

a. Unauthorised copyright photographic, audio or visual files, for example desktop wallpapers, MP3 files
b. Unapproved programmes or applications including screensavers, animations and games
c. Data or software that is defamatory, offensive, obscene, abusive, threatening, contains pornographic images, items covered by copyright law or any other illegal material.

DATA VISIBILITY

4.52 Security information (passwords etc) or other sensitive data should not be left unattended on a desk or other work environment and your screen should always be locked when you are moving away from your work area.

4.53 Whilst sharing screens on video conferencing and collaboration platforms additional care should be taken to ensure sensitive information cannot be viewed by unauthorised persons.

4.54 Before permitting remote access to IT support colleagues undertaking support and maintenance, care should be taken to ensure no personal/sensitive information is available on your desktop.

4.55 Individuals must ensure that any screenshots provided to initiate a support ticket or aid with troubleshooting a problem do not contain sensitive and confidential data.

EXTERNAL STORAGE DEVICES AND SERVICES

4.56 The use of USB storage devices is a common cause of compromise through infections from computer viruses, malware and spyware and should be avoided.

4.57 USB storage devices which are not from a trusted source must not be attached to an HHP computer.

4.58 Files on trusted USB storage devices must be scanned with an anti-virus product before use or transfer to HHP systems and network drives.

4.59 Staff must not use OneDrive on personally owned devices to access HHP accounts as this systematically synchronises all HHP data to that device, instead, documents residing in OneDrive should be accessed only via a browser.

WIFI

4.60 Public Wi-Fi connections, such as those in hotels and coffee shops, may not be secure. Checks should be made to ensure that you have the correct network name and credentials before you attempt to access.

ARTIFICIAL INTELLIGENCE

4.61 No form of sensitive or confidential data should be entered into an external AI platform.

4.62 It is the responsibility of those using generative AI systems to ensure that the system they use is approved and that the system is being used in a protected state.

DETECTING CYBER SECURITY EVENTS

5.1 All breaches and potential breaches are to be reported immediately (to Corporate Resources), and anyone raising such an incident will be treated positively and fairly for doing so. Any suspect device should be disconnected from the network and switched off immediately.

5.2 Our system are protected from attack through the use of firewalls; web traffic and email filtering/quarantining systems; real-time antivirus and anti-malware systems; device management tools; patching management; and threat and software vulnerability assessment software's.

5.3 Our systems allow us to identify inward and outward data traffic; users requesting data, and when; external sites accessed; strange data patterns; software vulnerabilities identified; best practice configuration changes and more.

5.4 These systems automatically update and respond in relation to industry best practices and guidance, others are not and rely on human review and action.

5.5 We will ensure that all event log data is backed up and kept safe from amendment or deletion.

MINIMISING THE IMPACT OF CYBER SECURITY INCIDENTS

6.1 Any response will be undertaken in conjunction with and documented in our Business Continuity policy and Cybersecurity Playbook, with the support of our insurers, ICT support providers and other external agencies as required.

6.2 An incident response will require significant information gathering on the circumstances and nature of the incident, including from users, support providers and other forensic data investigators. This will include the following questions:

i. What problem has been reported, and by who?

ii. What services, programs and/or hardware aren't working?

iii. Are there any signs that data has been lost? For example, have you received ransom requests, or has your data been posted on the internet?

iv. What information (if any) has been disclosed to unauthorised parties, deleted or corrupted?

v. Have your customers noticed any problems? Can they use your services?

vi. Who designed the affected system, and who maintains it?

vii. When did the problem occur or first come to your attention?

viii. What is the scope of the problem, what areas of the organisation are affected?

ix. Have there been any signs as to whether the problem has occurred internally within your organisation or externally through your supply chain?

x. What is the potential business impact of the incident?

6.3 The initial response team should be identified ahead of any actual issue so that it is in a position to move quickly. It will need to have the skills and knowledge required to decide on the response actions required, including the prevention of further harm.

6.4 To maintain robust ICT security and operational resilience, critical roles and responsibilities must not be assigned to a single individual. Duties should be

distributed across multiple staff members to ensure appropriate oversight, reduce risk, and maintain continuity of service.

6.5 As stated in our ICT strategy, we have redundancy and backup systems for all our critical systems, separated and ring fenced from our normal networks as much as possible, so that, even at a reduced capacity, we can continue to provide service.

REPORTING

7.1 Key cyber-security performance indicators will be reported to our Management Team and Board. Microsoft Secure Score or KickSecure Score are examples

7.2 All cyber security incidents will be reported to the Executive Team and Board and will inform future lessons learned processes and subsequent analysis.

7.3 It should consider the incident in relation to reporting, roles, governance, skills and organisational policies, processes and procedures as well as technical aspects of network and information systems.

INTERPRETATIONS & ABBREVIATIONS

The following interpretation and abbreviations are used in this policy:

WORD	INTERPRETATION
HHP or Partnership	Hebridean Housing Partnership
Board	Means the Board of the Hebridean Housing Partnership
Board Members	All Members of the Board including co-opted Members
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
Cyber-Essentials	A UK government-backed certification scheme that helps organisations protect themselves against common cyber attacks by implementing basic security controls.
KickSecure	A tool provided by Kick ICT Ltd for evaluating an organisation's ICT security position.
AI	Artificial Intelligence systems, and the use of structured collections of data used to train, validate, and test these and machine learning (ML) models
Wifi	A facility allowing computers, smartphones, or other devices to connect to the internet or communicate with one another wirelessly within a particular area.
Cloud	A method of hosting websites and applications on external 3rd party networks, comprising of virtual and physical servers - often drawing computing resources from a shared pool rather than a single server.
Phishing	The fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, or to ask for payment of invoices etc.

WORD	INTERPRETATION
Patches	A software patch is a small update to a program or operating system that fixes bugs, security vulnerabilities, and performance issues. It's a small piece of code that modifies the existing software to correct a specific problem, rather than a full version update. Patches are crucial for security, preventing unauthorised access and attacks that exploit flaws in the software.
Firewall	A firewall is a security system that monitors and controls incoming and outgoing network traffic to protect a computer or network from unauthorised access.
All references to the masculine gender in this policy shall read as equally applicable to the feminine gender	

APPENDIX 1

LEGISLATION PERTINENT TO THIS POLICY:

- Copyright, Design and Patents Act 1988
- Computer Misuse Act 1990
- Regulation of Investigatory Powers (Scotland) Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information (Scotland) Act 2002
- Public Records (Scotland) Act 2011
- Counter-Terrorism and Security Act 2015
- The Data Protection Act 2018
    - Network and Information Systems (NIS) Regulations 2018
- Telecommunications (Security) Act 2021
- Product Security and Telecommunications Infrastructure Act 2022