ELDONIAN

Business Continuity & Resilience Policy

Doc No: P002

Version No	Title	Author	Draft Date	Approved By	Approval Date	Live Date	Review Date
N/A	Business Continuity Plan	P Latham	Jan 2024	Board	Jan 2024	Jan 2024	Jan 2027
N/A	ICT Business Continuity & Resilience Policy.	P Latham	Aug 2024	Board	Aug 2024	Aug 2024	Aug 2027
1	Business Continuity & Resilience Policy	P Latham	October 2024	Board (based on previous approvals)	N/A	October 2024	Jan 2027

1. Introduction

This policy seeks to set out Eldonian Community Based Housing Association's (ECBHA's) policy positions regarding business continuity and resilience and associated approved planning. It includes the approved approach to keeping its ICT resources secure and resilient including planning the event of a cyber-attack.

This policy has brought together a number of previously separate polices into one document, Those previous documents and applicable content are superseded by this document.

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.

The plan for addressing a cyber attack is outlined in Appendix 1 of this policy.

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 ICT 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 Wider Disaster Recovery Positions

ECBHA will have a prepared Business Continuity Plan (BCP), this is outlined in Appendix 2.

The BCP sets out the intended approach to take in the preparation for, and management of, significant business disruption. The aim is to ensure critical business functions are maintained or resumed with minimum delay and minimal adverse impact on customers, the business and the organisations reputation.

The BCP seeks to provide a plan for strategic, tactical and technical capabilities to respond to incidents and business disruptions to an acceptable, pre-defined service level and compliance requirements. It also offers potential guidance and options to less serious incidents.

This BCP seeks to address all ECBHA operations. There are separate disaster recovery provisions, referenced in this plan, relating to the organisations IT infrastructure and software. In addition, it is recognised that there may be additional service or customer specific continuity provisions needed in relation to Robert Lynch House & Sibert House older peoples housing.

The BCP has been developed around the four themes of:

- People – staff, customers, the public
- Processes – both analogue and digital
- Premises – homes, offices, localities
- Providers – contractors, suppliers and partners

The main objectives of this Plan are to:

- Ensure the safety of all customers, staff and visitors is considered and prioritised
- Ensure that the pathway to recovery is clear and implemented as quickly as possible
- Minimise the disruption to normal operations

- Limit the extent of disruption and damage
- Minimise the economic impact of the interruption
- Proactively establish alternative means of key operations in advance
- Ensure that critical activities can be recovered within the recovery time objectives
- Ensure that a framework and structure exist for any predicted decision making, during times of disruption.

5 Review

This policy will be reviewed at least every three years and represented to Board for approval. It may be reviewed or amended beforehand in responses to incidents, best practice and changes to the operating environment.

Appendix 1 – Cyber Incident Response Plan

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.

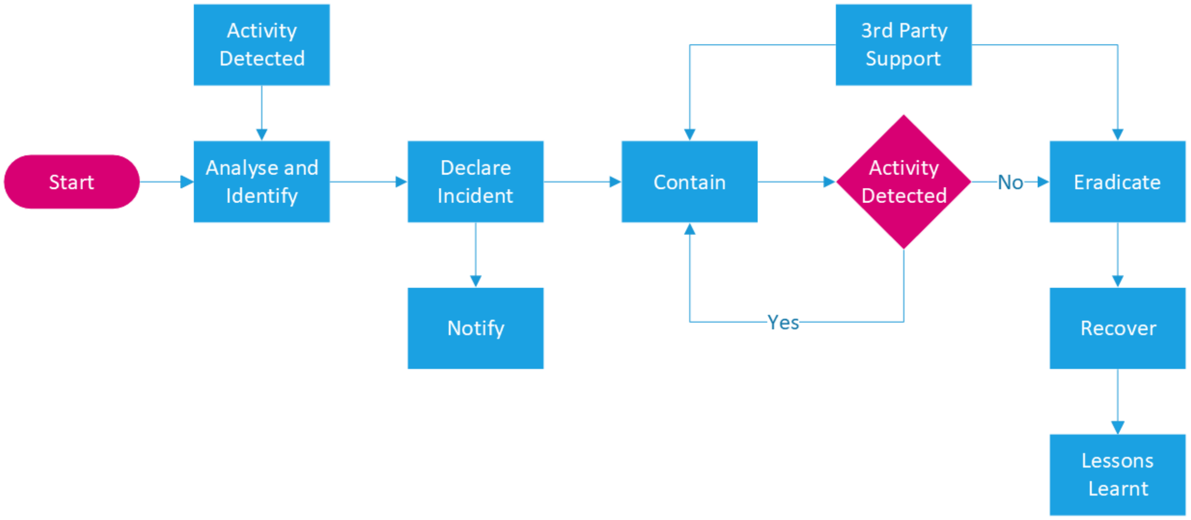
This approach is intended for incidents that involve confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out, for example:

- 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

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.

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?

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.

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.

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.

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

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

Cyber Incident Response – Golden Rule

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

Appendix 2 – Disaster Recovery Plan

This plan sets out the approach Eldonian Community Based Housing Association (ECBHA) intends to take in the preparation for, and management of, significant business disruption. The aim is to ensure critical business functions are maintained or resumed with minimum delay and minimal adverse impact on customers, the business and the organisations reputation.

Assumptions

The BCP is based upon the following key assumptions:

- **People**

Whilst the loss of some staff is assumed to be covered by deputisation, succession planning and external resources, the plan assumes that the majority of staff will be available for the recovery process.

Emergencies which impact on employees, their families or homes could reduce availability. However, in these circumstances, ECBHA will consider other options, including:

- Suspension of non-essential workloads in order to transfer staff
- Offering any part time staff additional hours
- Use of agency staff or specialist organisations
- Mutual support if available from other Registered Providers
- Additional hours for available staff

Events that cannot be addressed through a combination of these options are likely to be considered ‘Overwhelming Events’ defined in section 3.5.

- **Processes**

From an IT system and digital processes perspective it is assumed that the back-up process meets the defined needs of the business in terms of recovery of online systems and data to the appropriate retention point and within an adequate recovery timescale.

It is understood that aspects of the ECBHA utilises off premise ‘cloud based’ server hardware. It is assumed that the back up arrangements are able, at least for an agreed period, to enable data to be accessible to the wider organisation and digital processes to operate, for example customer portal, until the main provision can be resumed.

ECBHA specifies its retention and recovery timescale requirements in its arrangements with its IT service and software providers. These requirements will be recorded within the Disaster Recovery Arrangements (DRA).

Any electronic data that is required for recovery is assumed to be recorded in retained network drives and SharePoint, rather than on local drives (including laptops) which are not backed up.

- **Premises**

It is assumed that office disruption, an incident that affects the Office at The Tony McGann Centre, Eldonian Village, Burlington Street, Liverpool, L3 6LG. will not affect the housing stock at the same time, with the possible exception of severe weather.

- **Providers, Suppliers and Partners**

It is assumed that as part of its supplier approval practices, ECBHA ensures that all business-critical providers, suppliers, contractors, and partners have their own suitable business continuity plans in place.
It is also assumed, that in most situations, while ECBHA may be experiencing a significant or critical event or incident most of its suppliers and partners are unlikely to be affected.

Overwhelming Events

However comprehensive the ECBHA is, an event may occur which exceeds ECBHA's ability to recover using the resources available to it. In this situation a decision will be made regarding the future of the business, which may or may not be restored. Such a situation would be considered an 'Overwhelming Event' (OE). The decision to call an OE sits with the Leadership Team and/or the Chair and will likely be influenced by advice from other outside parties such as Police, government, or the regulator for example as the enormity and impact of an OE unfolds.

It is assumed that during the emergence and duration of an OE the immediate priority will remain the safety of life for which the information contained within this BCP is anticipated to be applicable, either fully or in part. An OE is likely to require a bespoke plan developed in conjunction with other parties involving the Board and Leadership Team.

Critical Activities

ECBHA is a community housing association providing circa 400 quality affordable homes in the Vauxhall area of Liverpool.

In respect of business continuity its critical activities are considered to be:

- **Customer Service:** Ensuring an access point for communicating with residents and other external parties. Attending to urgent and emergency repairs.
- **Housing**: Letting homes, urgent estate management, monitoring and collection of rents, tenancy management including addressing anti-social behaviour and safeguarding concerns.
- **Older Peoples Housing:** Ensuring safety of vulnerable residents.
- **Assets**: Ensuring health and safety and statutory testing compliance.
- **Finance:** Payroll, processing supplier payments, rents processing and reporting.
- **HR:** Ensuring the availability of the right people resources to respond to the incidents.

The above activities are supported by colleagues, systems, and third-party partners. During a business continuity incident support from these will potentially become critical, particularly relating to IT / digital service delivery and internal / external communications.

While many roles are undertaken by multiple individuals or can be carried out by staff with transferrable skills, there are some niche specialist roles that are carried out by individuals that directly or indirectly have implications for critical activities. ECBHA will proactively identify and consider these roles within its structure and have considerations in place that will aim to support continuity.

If a continuity incident is prolonged, other organisational activities may become critical over time, for example if the incident significantly hinders progress of a development or the ability to compete a required regulatory return is affected.

In the event of an incident affecting ECBHA, non-critical activities may be suspended, and resources allocated to supporting the maintenance and recovery of critical activities. Non critical activities will then be resumed at the earliest opportunity.

Other topics to consider in the restoration of 'normal' services include:

- Protection of staff, customers and visitors
- Contact with customers, suppliers, and other stakeholders to provide updates on ECBHA’s status and capacity.
- Control of the flow of information about an incident
- The communication to all staff of immediate contingency arrangements
- Setting up temporary facilities and arrangements necessary
- Recreating records and recovering or protecting files and documents
- Securing original documents

- Rebuilding IT / digital systems, restoring data and making the systems available to in-house and remote users, in the stated timescale
- Re-establishing premises or creating new premises
- Establishing any insurance claims

The Plan is structured to deal with incidents that affect the following areas and resources, either singly or in combination:

- People – staff, customers, the public
- Processes – both analogue and digital
- Premises – homes, offices, localities
- Providers – contractors, suppliers and partners

To ensure the maximum flexibility, it is not based around the response to specific scenarios but looks at the effects any incident might have.

Incident Definition

An incident may be any situation which might or could lead to a disruption, loss, emergency, or crisis affecting the normal operations of ECBHA. Examples may include loss of ICT systems, loss of data, fire or flood resulting in loss of a building, loss of a key supplier, pandemics / epidemics or weather-related incidents.

Disruptive incidents occur on an almost daily basis. It is important to establish at what point a disruptive incident should be escalated to invoke the BCP.

The relevant member of the Leadership Team will assess the nature and extent of a disruptive incident and its potential impact on the services of ECBHA when taking into consideration the decision whether to invoke the Plan or deal with the incident as part of 'business as usual'. In considering the invocation of the plan, ECBHA should keep in mind the likelihood of a minor emergency having the potential to worsen and escalate.

The table in Appendix A may be used to assist in the decision whether to invoke, or not. However, depending on the nature, scale and location of an incident, it may be clear that the BCP should be invoked.

Incident Detection

Incidents and events that present a business continuity risk can present from a multitude of perspectives, routes and can range from significant one of issues occurring rapidly through to a number of smaller issues that combine to create a larger threat or a smaller issue that becomes more significant over an elongated timeframe. This makes a single channel for detection difficult.

ECBHA encourages open and accessible communications to ensure that customers, staff and third-party suppliers and contractors are encouraged to raise concerns as early as possible. More often than not these are unlikely to be of a nature or of significant enough size to pose as business continuity threat. However, ECBHA seeks to empower colleagues to escalate issues with impact beyond their remit to the Leadership Team.

Business continuity incidents are likely to impact some or all the organisation's critical activities.

ECBHA has in place contracts with out of hours service providers. These providers are equipped with the appropriate contact information regarding senior duty staff to escalate incidents posing a business continuity risk as early as possible.

Incident Response

Each incident will be unique in nature and consequently may involve a multi-agency response from emergency services, therefore the response from ECBHA must be flexible to be able to adapt to these changing and demanding circumstances.

In the event of a major civil incident, the relevant Local Authority and / or Emergency Services plans would be activated. ECBHA would cooperate with the Local Authority and Emergency Services as required in these circumstances. This may necessitate ECBHA allocating staff to attend Local Authority Emergency Rest Centres in order to address the needs of ECBHA customers who may have been temporarily relocated there.

The Leadership Team shall meet as regularly as necessary for status reporting and debriefing and not less than every 24 hours during the first 5 days of a major incident occurring.

All staff involved in responding to the incident must keep a full record of any communications, actions or decisions. These records may be used as part of the post incident debrief and will be kept for a period of no less than three years, should they be required for any further investigation / litigation / review purposes.

Fire and Emergency Evacuation Plans

The organisational fire and emergency evacuation plans will be used and are not compromised or superseded by this document. A summary of the emergency evacuation plans is on display at various locations on each site. Copies of the plans for each site will also be kept remotely for flexible supply to emergency services if necessary, during an incident. These will be kept on the encrypted USB stick with BCP members Grab Bags as outlined in Section 8.

Site Closure

- **Partial Closure.** In the event that only parts of a premises are affected by an emergency situation, it may be decided by the Leadership Team to continue some presence at the affected premises. However, this will only be where:

  - Emergency services (if involved) recommend there is no further danger
  - The insurance company agrees to this from the perspective of cover and any applicable claim
  - Safe access / egress can be maintained
  - Data / information security is not at risk
  - Heating, lighting, sanitation etc are available

  - There is adequate containment (fire or security doors etc) from the damaged areas and compliance requirements can be achieved.

- **Full Closure.** In severe incidents, the emergency services may require the closure of a premises.

  Where this decision is made during working hours, the appropriate members of the Leadership Team will request staff work from home, or from another appropriate venue. Where closure is initiated out of hours, the Leadership Team will organise appropriate notification to staff via an appropriate cascade of calls, email, SMS, or social media.

  Should the remote situation occur that it is not safe or practicable for staff to return home ECBHA will endeavour to secure a suitable safe temporary location to accommodate staff.

- **Residential Accommodation.** In the event of the partial or full closure of residential premises affecting the homes of ECBHA's residents, ECBHA will, seek to secure appropriate hotel accommodation for affected individuals for the initial night. Should the closure of the premises be extended further, ECBHA will work in conjunction with the local authority to secure appropriate temporary accommodation.

  ECBHA is particularly aware of the need to ensure that there is an emergency location for vulnerable residents, particularly those that are older, should their accommodation be affected. Vulnerable residents affected by an incident, in the first instance will be offered emergency relocation to the communal facilities at Robert Lynch House.

  If Robert Lynch House is not available due to the incident, then the ground floor of Tony McGann Centre can be used for smaller numbers, and potentially Eldonian Village Hall or Eldonian Care Home for larger numbers, subject to confirmation from the operators of suitable availability / capacity.

  A member of ECBHA staff will be based at the selected location to provide refreshments, updates, assurance and to liaise with other agencies regarding individuals as appropriate. Where necessary additional staffing, volunteers and resources will be authorised as part of the incident response management to ensure emergency arrangement remain effective in safeguarding vulnerable residents.

Public access

Where expected, visitors will be contacted by staff to notify them of any closure / restricted service and any alternative arrangements. Staff who have made appointments will contact their residents and other guests to either cancel or reschedule appointments, as necessary.

Security Arrangements

Where it is not possible to secure the building by normal means (alarms and locks) owing to the nature of the damage, ECBHA will liaise with the emergency services / suppliers and consider:

- Boarding up / sealing of potential points of entry (windows, doors etc)
- Engagement of security staff to guard the premises

As soon as practically possible, while ensuring the safety of staff and contractors and any immediate other factors, such as crime scene implications are also considered.

Incident Management Control Centre

During critical incidents and overwhelming events an Incident Management Control Centre (IMCC) will be established to provide a central hub for activities and decision making. The location of the will be the Meeting Room at Tony McGann Centre, or a suitable location identified by the Leadership Team. If during the incident there is confidence that IT /digital systems will remain secure the Leadership Team may opt to define a virtual IMCC location.

How the Business Continuity Plan is invoked.

The emerging potential business continuity threat is more than likely to be escalated internally to a member of the Leadership Team as a critical incident. It may also come through a third party such as emergency services. Colleagues and out of hours contractors will be proactively prepared for such third-party notifications.

Invocation of the BCP is the responsibility of any member of the Leadership Team. They must take a view on how the incident that has occurred may impact on the critical activities of ECBHA. If they ascertain that the incident, or a combination of concurrent incidents together form a substantial continuity risk then the BCP should be invoked.

Invoking the BCP commences with a notification to the Business Continuity Team (BCT), the membership of which is listed in Appendix B.

Assessing Information

The first task of the BCT is to familiarise itself with the information available in order for it to be prepared for its decision making responsibilities. It is important that the BCT seeks rounded information on the threat and is objective about the importance and reliability of the information it is being provided. As the BCT will have the visibility of the situation, other staff should not make decisions arbitrarily, unless this authority has been specifically delegated to them by the BCT. During and in the immediate aftermath of an event the flow of information may be confusing, and a system is required to prioritise this information and assess its reliability.

The table below provides a structure for prioritising incoming information during a critical incident:

		Importance		
		Level 1	Level 2	Level 3
Reliability	High	Critical	Important	Noted
	Medium	Important	Relevant	Noted
	Low	Relevant	Relevant	Noted

Importance:

- Priority Level One — direct, immediate impact on staff and operations
- Priority Level Two — indirectly impact on operations
- Priority Level Three — no impact on the operations

Reliability

- High — same information from two or more direct sources.
- Medium — information from one direct source, internet, television or radio.
- Low — information from an indirect or uncorroborated source.

All decisions, reasoning behind them and available information that the decision was based on should be recorded in an activity log for the post event review.

Communication

Effective communication is essential to an effective response. The incident should be evaluated and the impact on a variety of communications streams e.g. email, mobile voice networks and social media anticipated. All streams should be constantly assessed, with alternatives understood.

An incident can be passively monitored through broadcast and online news streams and social media. Staff should direct any information that they have about the incident to the relevant Leadership Team member who will bring it to the attention of the BCT.

The BCT is responsible for approving communications and will discuss and agree on the key messages to be distributed to staff, intermediaries, residents and the public generally. Under no circumstances should messages be released unless it has first been approved by the BCT.

All incoming / outgoing communications should be recorded in a communications log.

It is the responsibility of each member of staff to ensure they have the personal contact details for those within their department. Personal information should be held in accordance with data security policies.

It will be the Executives responsibility to ensure the Chair of the Board is kept fully informed. They in turn will update other Board members.

Appropriate members of the BCT will be responsible for contacting all key groups and interested parties. Information received from national, regional or local advisory systems will be documented within the Communications Log.

ECBHA should, if necessary, appoint an emergency services liaison to deal with emergency services responding at the affected site.

In the event of an incident that has caused a significant impact to the operations of ECBHA or may be perceived as having done so (e.g., an incident in the local area), the following methods of communication should be utilised:

- **Website —** the front page amended with the nature of the incident, its impact on the operations of ECBHA and the response that is underway. The message is to be reviewed by the BCT prior to publicising. This message should include a telephone number through which any concerned members of staff, friends or family can contact the organisation for further information if appropriate.

- **Telephone** — inbound calls may not be able to be answered during an incident, Whenever possible message should be provided to inform incoming callers of the situation with details of emergency contact arrangements.
- **Email** — email system should in most circumstances remain functional. When necessary, an auto response should be put on all email accounts acknowledging that there has been an incident, directing people to the website for up-to-date information.
- **Social Media** — Use of social media needs to be carefully managed, however it also provides an effective for mass communication that may be appropriate to some incidents and events.

In the event of public or media interest, enquiries should be referred to the BCT. Until an approved statement can be provided, communication should be restricted to:

- confirmation of the obvious
- confirmation that the welfare of staff and stakeholders is the priority
- cause and effect are under investigation
- implementation of the organisation's contingency plan is in progress
- a detailed statement will be provided as soon as possible.

Press releases will be composed by the BCT.

The spokesperson for the organisation is the CEO or appropriate person acting as a successor. No other member of staff is authorised to speak on behalf of ECBHA unless designated to do so by the CEO or Chair.

Roles and Responsibilities

Business Continuity Team – Responsibilities

BCT responsibilities may vary slightly depending on the nature and scale of an incident, and may include:

- Investigate circumstances of the incident and establish close links with emergency services
- Coordinate the recovery of operations
- Notifying and liaising with the Board

- Coordinate communication with all stakeholders, including:
    - Develop a recovery strategy
    - Communicate with staff, including instructions regarding remote working
    - Approving and collating all spending on the incident
    - Liaise with insurers / loss adjusters
    - To decide when the incident has diminished sufficiently to stand down
    - Post incident review

BCT members will be provided with a 'grab bag'. Members should keep the grab bag in a secure and accessible location that is not within a ECBHA office. The content will be reviewed annually to aid delivery of the role. The initial anticipated content includes:

- Hardcopies of:
    - Business Continuity Plan
    - Disaster Recovery Plan
    - Out of Hour Contractor Arrangements & Contacts
- Encrypted USB with:
    - Business Continuity Plan
    - Disaster Recovery Plan
    - Bank Details
    - Out of Hour Contractor Arrangements & Contacts
    - Contractor Contact Details
    - Local Authorities Contact Details
    - IT Provider Contact Details
    - Insurance Details
    - Housing Stock List
    - Fire evacuation plan for each premises (where in place)
    - Floor Plan(s)
    - Inventory of Staff Skills / Staff Geographical Locations (Work/Home)
- Torches
- High visibility vests
- Foil Blankets
- First aid kit
- Universal mobile phone charger

Recovery & Resuming Activities

- **People.**

The immediate issue to address will be to confirm the well-being of all customers, staff and contractors to ensure that they are safe, have the ability to get home and to get into their homes. To assist with this, remote workers are issued with lone worker alarms.

A major incident may unfortunately lead to immediate casualties including fatalities amongst ECBHA customers and staff. Where there is a nominated next of kin for a customer or staff member ECBHA will notify that next of kin that an injury has occurred and where the individual is receiving treatment. In the event of fatalities, emergency services are responsible for notifying the next of kin contact. In no circumstances should ECBHA staff make this first contact unless explicitly directed to by the emergency services.

Should some roles not be covered as a consequence of continuity incident the organisation will consider how best to deploy the resources that are available to focus on the delivery of critical activities. In some instances, for example niche specialist roles, or those requiring volumes of staff, contractors and external agencies can cover.

There is a succession plan for the BCT members to ensure the decision-making authority for the Business Continuity Plan is uninterrupted. Details are in appendix B.

Communication with staff is key following an incident and contact details should be available 24/7 outside of the IT / digital network.

Beyond the initial period ECBHA will arrange pastoral care, liaising with injured staff and their families, and the arrangement of grief and trauma counselling. Specialist advice may be required as part of the recovery process and consideration should be given to co-opting such advice to the BCP where appropriate.

Processes

Information, Data & IT.

A separate recovery plan is in place to address the technical recovery and availability of information and data alongside the IT/digital business systems that utilise it. Telephony arrangements are included within the disaster recovery plan.

Manual systems

As a legacy of the pandemic and the growth of hybrid working there are reducing numbers of manual systems and processes within ECBHA, and this trend is expected to continue. However, during and following a continuity challenge there may need to be additional manual systems implemented to overcome issues of IT/digital provisions not being available. The aim is for these to be minimised and kept as simple as possible to deliver critical activities only. As soon as there is scope for these to revert to the online this should be progressed. Manual systems should also be proportional to the volumes of transactions expected during the continuity incident.

Where additional manual systems are needed in the short term, there must be a balance achieved of ensuring suitable probity, enough detail to enable audit while not being unduly onerous for customers, staff, or contractors.

Instances may occur where business as usual manual systems are not accessible, or files / folders may be destroyed. These manual systems will already be documented and the BCT will need to:

- Acknowledge when due to an incident they may not be available or disrupted.
- Consider if they can be suspended while the incident is addressed.
- If not, then draft a pragmatic short term alternative manual process.
- Acknowledge where customers may be disadvantaged and highlight this to be addressed as part of the 'return to normal' activities.

It is imperative that any interim manual processes are proportional and realistic, particularly during an initial response, but also recorded for future reference. Interim manual processes should be approved by a BCT member.

Finance

The organisations credit cards are considered the most flexible method of payment should emergency purchases be required to address a business continuity threat. However, in some instances it may be appropriate to make purchases from suppliers that ECBHA already has established business relationships with that can be flexible in terms of procurement should the usual purchase order / invoicing arrangements be disrupted.

Purchasing authorised by the BCT during a continuity threat must be appropriately logged and receipts retained whenever feasible.

Payroll is a key process for staff, with payroll run every month across the organisation. As a worst-case scenario, the file from the previous month would be re-run adjusting for known joiners and leavers and amendments can then be made in the following pay period as necessary should the continuity challenge have been resolved.

Most outgoing payments made by ECBHA are via BACs. If a continuity challenge prevents ECBHA having access to BACs the organisation will seek to contact all suppliers with payments due to explain the situation and, if possible, the scope of delay. If ECBHA is unable to make BACs payments for over 5 working days alternative methods of payment to contractors and suppliers will be explored and implemented.

Rent payments are likely to be unaffected if the IT/digital systems are unavailable but reconciliation to customer accounts will be delayed. While this would not be an immediate challenge to critical activities any more significant delay could impact on cash flow and needs to be closely monitored by the BCT.

Premises

Any premises or environments will only be used once ECBHA is confident that they are sufficiently safe and secure to do so, this includes both homes and business premises.

In considering premises for business activities, the following locations are specified:

Primary	Tony McGann Centre Offices
Secondary	Robert Lynch House Offices & Communal Rooms
Back Up 1	St Giles Close Community Room
Back Up 2	Eldonian Village Hall (in agreement with Eldonian Leisure Ltd)
Back Up 3	Eldonian Care Home (in agreement with care provider)

Due to ECBHA's hybrid working provisions ECBHA is confident that that an incident that puts business premises out of use would be unlikely, on its own, to present a significant business continuity challenge.

In such circumstance homeworking or relocation to an alternative ECBHA location as defined above would be expected. If the office arrangements are unavailable for a significant period short term meeting space would be sought.

There is little exposure to consumables that cannot be readily replaced. Office supplies, equipment and furniture can be replaced with minimal impact.

Organisation credit cards could be used for small purchases and limits can be varied should flexibility be need during a business continuity challenge at the authorisation of the BCT.

Providers

There are several critical suppliers used by ECBHA. If applicable following an incident, they will be contacted by an appropriate member of the BCT. Contact details of some key suppliers are provided on the encrypted USB stick in BCT members Grab Bags.

The loss of a key site will mean that couriers and Royal Mail will not be able to deliver post. Should contact the local sorting office not be possible then contact Royal Mail External Relations Team, inform them of the situation and request that mail is held at the sorting office for collection. The person sent to collect the mail will carry a letter of authorisation to do so.

Return to normal

The organisation will restore and return business operations from the temporary measures adopted to normal delivery at the earliest opportunity following an incident.

The decision on how best to 'return to normal' will need to be taken by the CEO and will be based on the severity of the damage caused by the incident and estimates.

of how long it might take to re-establish the necessary facilities.

A return to normal should include provision for the resumption of all business activities, not just those identified as critical.

It may be that based on the impact of the incident and the responses that a potential new 'normal' may emerge and be desirable. If this amounts to a strategic change, then working towards this defined 'new normal' will require a Board approval, however seeking this should be expedited to prevent undue delays in the organisational recovery.

Standing the Plan Down

BCP's are anticipated to have a lifespan of up to three months during an incident. This is considered sufficient time for most service delivery to be re-established and the critical threat to continuity to have passed or been resolved. This does not mean that previous 'normality' will have been fully restored, for example if a building needs replacement, however instead robust workarounds have been established for the interim and the impact can now be addressed within day to day activities.

The decision to stand the plan down is taken by the BCT.

Once the plan is stood down, all the information used during the response to the incident should be collected and stored safely. A post incident review should occur to assess the success of the plan, using the information contained within the activity log. The lessons learned will be used to update the BCP and will be reported to Board along with a summary timeline of the incident, an overview of how any customers may have been disadvantaged and any proposed actions to address this.

Plan Training and Testing

Exercising will be undertaken on an annual basis to test the plan and the lessons learned fed back into the BCP development.

Exercises will involve BCT members and consideration will be given to including other staff as and where appropriate.

All new staff will receive business continuity awareness raising as part of the induction process and existing staff will receive regular refresher training with any updates highlighted.

The BCP will be updated following any lessons learnt from exercises or incidents or upon three years since its previous review. Reviewed BCP's will be approved by the Board. In addition the appendices should be updated upon changes of BCT members or succession arrangements

Appendix A BCP Invoke Decision Tool

It can sometimes be unclear if a situation is challenging operating matter or if the situation can be considered to have escalated to being a more substantial business continuity threat. This tool is aimed to support senior leadership in decision making. Scoring is not intended to be totalled and certain scores create triggers as business continuity threats are rarely simple to quantify, however the responses are intended to provide focus at a potentially charged and fact moving time. However, generally more higher scores occurring will provide a stronger case for invoking the BCP . It can be completed and then reviewed and revised as a situation changes.

There are seven key themes:

- Level of emergency / threat to life
- Property
- People
- Process including IT/digital services
- Providers
- Finance
- Communications

		Selection	Selection	Selection
Date /Time				
By				
Level of Emergency / Threat to life	Score			
No immediate emergency / threat to life	1			
Emergency requiring limited emergency responders and is not expected to pose a threat to life	2			
Emergency requiring limited emergency responders and/or has the scope for lives to be in danger	3			
Significant emergency requiring multiple emergency responders and/or substantial number of lives in danger	4			
Property				
No damage to property assets	1			
Limited damage to a property asset that does not put it out of use as homes or workplace	2			
Substantial damage to a property asset or that puts it partially out of use as homes or work place for a small number of people	3			

Extensive damage to a property asset that puts it fully out of use preventing it being used as homes or work place for a significant number of people	4			
People				
All expected staff are available	1			
A limited number of staff are not available but with some re-deployment services can be maintained	2			
A limited number of staff are not available but these include some crucial roles and skills that cannot be addressed through re-deployment to maintain services	3			
Substantial numbers of staff are not available having significant impact on the ability to maintain services	4			
Process including IT/Digital Services				
All manual and digital processes are available and expected IT access available	1			
There is some localised disruption to a small proportion of business processes and reasonable alternative delivery methods can be implemented within a short timeframe	2			
There is substantial disruption to some significant business processes and there are limited alternative delivery methods that can be implemented within a short timeframe	3			
IT/Digital process are off line, substantial data loss preventing delivery and/or there is substantial inability to deliver manual processes	4			
Providers				
Suppliers, contractors and providers are delivering services as expected	1			
There is some limited disruption to a smaller number of supplier contractors and providers but alternative sources can be arranged within a short time frame	2			

There is more significant disruption to a number of, or key suppliers that is requiring them to invoke their business continuity / disaster recovery arrangements and/or the arrangement of alternative supply is limited	3			
There is significant rapid disruption to the overall supply chain across several areas of the business that the arrangement for alternative supply is significantly limited.	4			
Finance				
Financial operations are operating as expected	1			
There is some limited disruption to financial operations but key delivery can still be achieved	2			
There is disruption to financial operations that will prevent some key delivery to be achieved	3			
There is substantial disruption to financial operations that will impact the organisations' ability to meet its financial commitments.	4			
Communications				
Communication operations operating as expected	1			
Limited communication disruption and sufficient alternative communication options available, and/or some limited press enquiries regarding the situation	2			
More substantial communications disruption that is potentially preventing some staff / customers making sufficient contact, and/also there is a growing PR / Press situation that has the potential to be damaging	3			
Significant disruption in communications with staff and customers and/or fast moving and damaging PR / Press situation	4			

Appendix B Business Continuity Team Members

Members are listed in order of seniority for BCT purposes. The most senior member available will take responsibility for chairing the BCT unless agreed otherwise between members due to the nature of the incident.

It is expected that the BCT will seek to make collective decision making to ensure a rounded, proportionate response. However, it is acknowledged that the BCT will need to make some rapid decisions and therefore its chair may need to make decisions if a collective consensus is not achieved in a timely manner.

The ECBHA Chair or Deputy Chair will have oversight of the BCT activities and will liaise directly with the BCT chair only to ensure a clarity of communications and to ensure the wider BCT is directed towards the incident response. Some strategic BCT decisions may need emergency/urgent ratification by the ECBHA Chair or Deputy Chair on behalf of the Board.

The ECBHA Chair or Deputy Chair will take responsibility for communication with the wider Board, notifying them of, and providing updates regarding an incident.

All Board members will be made aware of and be expected to have access to this plan in the event of an incident.

Roles	Primary Contact Number	Out of Hours Contact Number
Shirley Davies Chief Executive Officer	xx	xx
Graham Davies Chief Finance Officer	xx	xx
Michael Wood Chief Operating Officer	xx	xx
Peter Latham Business Improvement Manager	07450514264	07450514264