Purpose & Scope

The purpose of this policy is to set out Adullam's approach in the event of a natural or man-made incident or disaster either at a local project, area or national level. The scope of this policy covers business-critical activities delivered to all internal and external customers, and service delivery partners which includes (but not limited to):

- All Tenants, Residents and Service Users (TRS)
- All staff
- Contractors
- Partnership bodies
- Commissioners/Local Authorities
- Enforcement Authorities
- Regulatory bodies

The policy aims to deliver the following targets in the event of a disaster occurring:

- Temporary accommodation for Adullam residents will be secured within twelve hours.
- Front line support services will be resumed within twenty-four hours; and
- Central functions and services will be 50% capacity within 48 hours, 80% within five working days, and 100% within ten working days.

Business critical activities can be defined as:

"Critical operational or support activities without which the business would rapidly be unable to achieve its mission or objectives."

1.0 Objectives of the Policy

1.1 The objectives of this policy are:

- To improve the resilience of each central department within Adullam Homes through identifying and managing the many and varied operational risks inherent in the delivery of services to our tenants, residents and service users.
- To efficiently maximize the use of available resources during a serious incident/emergency/disaster to reduce recovery time; and
- Commit Adullam Homes to a yearly schedule of review for the business disaster recovery and continuity policy, BDCR departmental and local plans to ensure they reflect the operational needs of the Association and risk scenarios identified.
- Provide leadership, effective and clear communications.
- Continue the welfare and wellbeing of our staff, tenants, residents and services users.

1.2 A disaster is an event which immediately puts at risk all or a major part of the business-critical activities or loss of identified core services.

Business Critical Activities Include:

- Repairs and maintenance
- Housing management functions
- Support to our tenants, residents and service users
- Serious incident response
- Safe housing and workplace

Core Business Services Include:

- Loss of key premises
- Loss of key staff
- Loss of ICT/Data (digital and other)
- Loss of communications
- Loss of utilities

1.3 Similarly, a breakdown in external communications could also prevent us from carrying out our statutory or contractual duties. We therefore invest resources in ensuring that our Business Disaster Recovery and Continuity Plans are reviewed annually and at any particular scenario where a plan is triggered. BDRC events will be captured in our reporting mechanisms and discussed bi-annually for trends and or lessons learned. Particular themes of risk will inform the Association's Risk Register reviewed monthly by SLT and reported to Adullam's Board.

2.0 Business Disaster Recovery and Continuity Plans (Departmental and Local)

2.1 BDRC Plans allow for the effective management and assessment of identified risks, serious incidents, disaster scenarios which potentially might impact business critical activities.

2.2 Departmental and local plans are established focusing the Association's resources and response comparably to the incident level, emergency or disaster scenario encountered. The overall objective from these local and departmental plans is to provide for an orderly, well managed, effective, and timely recovery from any serious incident or disaster.

The Plan:

- reduces confusion during any chaotic period by a clearly defined course of action.
- establishes the person/s responsible for disaster recovery.
- identifies resources, assets, specialist contractors and support that can be utilised if necessary; and
- specifies the steps necessary to return to normal business in as short a time as possible.

2.3 **Roles and Responsibilities**

The overall responsibility for business disaster recovery and continuity arrangements across the Association is with the Chief Executive Officer. The Chief Executive Officer will ensure in that all staff will work together to restore business-critical activities and core services. In that the Association has sufficient BDRC plans to manage identified risks, audit pathway for continuous improvement and reporting mechanisms in place to establish the suitability and effectiveness of all plans, departmental or local.

Key staff will form 'four' teams structured to respond effectively and proportionately to the level of incident (1-3), emergency or business disaster recovery scenario.

Disaster Recovery Support Team - Local

This team will be responsible for:

- Communication with the Regional Recovery Management Team
- Assessing the incident and/or the damage incurred and allocation of resources
- Invoking the local disaster recovery plan and assembly of the Support Team
- Ensure recovery procedures are implemented correctly
- Advising staff/outside bodies as outlined in this document
- Prioritise staff, tenant, resident and service user welfare
- Undertake immediate health and safety considerations

Position	Name	Contact Information	Working Hours / Shift Pattern availability
Property Services & Operational Manager			
Team Leader			
TSO			
Service Co-Ordinator			
Concierge			

Disaster Recovery Management Team - Regional

This team will be responsible for:

- Communication with the National Strategic Management Team
- The implementation of the recovery plan - including redirection of phone calls
- Work continuity and critical business activities recovery

- Remedial work to ensure the project, office or site repairs are carried out in a timely manner
- Alternative arrangements should the office be offline for a prolonged period of time
- Redirection of mail
- Debrief of teams
- Post incident support and Welfare
- Monitoring the progress of any Quality Improvement Plan (QIP) or lessons learned

Position	Name	Contact Information	Working Hours / Shift Pattern availability
Regional Out of Hours Management Support			
Regional Manager			

Disaster Recovery Management Team (National Strategic) *

This team are responsible for:

- Ensure resources are allocated to enable the swift recovery of the functions within the project
- Initiative departmental Business Disruption Action (BDA) plans e.g. cyber security
- Release financial resources
- Measure the impact nationally (if applicable)
- Inform others in the Association and Board members
- Inform Association Insurers
- Health and Safety impact (if applicable)
- Inform Homes England (if applicable)
- Inform Civil Contingencies Officer (if applicable)
- The Local Management Team will update the National Team

Position	Name	Contact Information
Chief Executive Officer	Alison Sargent	07717 518794
Executive Director of Housing and Support	Ged Riley	07768 636956
Assistant Director Quality & Assurance	David Moore	07768 637055
Group Financial Controller	Harj Takhar	07773 482436
Assistant Director People	Ceri Murphy	07960614165

**** The National Strategic Team should be contacted regarding significant organisational wide issues which have met the BDRC definition. The final decision will be made by the allocated SLT lead.***

Disaster Recovery Departmental Support Team
Deployed at any level to meet national or local level planned response.

Position	Name	Contact Information	Working Hours / Shift Pattern availability
ICT Manager	Adam Anwari	07458054613	Mon – Fri 9-5
Asset Manager	Lyndon Wilson	07825 552690	Mon – Fri 9-5
Health & Safety Manager	Paul Wilkins	07458054613	Mon – Fri 9-5
National Housing Manager	Pauline Gooden	07557191854	Mon – Fri 9-5
Communications Manager	Sue Grief	07717485208	Part time 22.5 hours
Quality Assurance Manager and DPO	Phil Gardiner	07773 482549	Mon – Fri 9-5

2.4 All staff are responsible for ensuring that disruption is kept to a minimum in the event of a disaster.

2.5 A copy of the departmental plan and local plan should be kept in a place readily accessible by the identified responsible individual for services/sites and out of hours on call staff.

3.0 Risk Identification and Management in National and Local Plans

3.1 The identification of risks to the business-critical activities or core service is carried out as part of the standard risk analysis similar to that which takes place in the business Risk Register.

3.2 The departmental and local plans exist to mitigate the risks identified nationally or locally using appropriate expert knowledge and information/data available.

Risks - Examples but not exhaustive to:

3.3 **ICT Systems**

One of the most identifiable areas of risk is the loss of ICT systems. We use Microsoft Azure cloud storage. Adullam Homes servers are currently in a southwest location and have data replicating in Dublin where our other Microsoft server is located. All hard copy personal data for our tenants, residents and service users is stored on our Pyramid Performance Management Database.

The local backups are tested monthly for validation (or when a data restore job is required from the Group). Annual testing of the off-site replicated system is also

carried out by our MSP (managed service provider) in our disaster recovery (DR) environment that tests all production servers and connectivity.

All data generated by users and the system sits in a Tier 4 datacentre. Should there be a disaster at any datacentre in the UK, data would be replicated in advance to an EU Microsoft data centre. Therefore, the risk to data is low as it is hosted in co-locations.

Adullam have adopted a strict approach to Cyber Security, which implements strong encryption across all mobile devices including laptops, mobile phones and tablets. The encryption is industry standard.

3.4 **Large Scale Power Outages**

Power cuts from the National Grid for extended periods (planned and unplanned) in larger areas (i.e. not just one building but all properties in an area), affecting both staff at home and in work, and TRS.

3.5 **Fire**

One of the most identifiable risks to our properties is Fire. All our properties staffed and unstaffed are fire risk assessed on a regular basis in line with our Health and Safety Policy Fire Safety Arrangement.

3.6 **Threat to Life**

This could include incidents involving firearms or other dangerous weapons, where staff, TRS or customers are threatened, injured, or killed. This could also include hostage situations.

3.7 **Pandemic/Epidemic**

Can lead to a significant drop in staff numbers and our ability to maintain essential business activities or core services.

3.8 **Severe Weather**

This would include sustained periods of adverse weather resulting in breakdowns in the transport network, staff availability, and effects on other infrastructure and properties (power/floods, etc).

4.0 Initiating National and Local Plans

4.1 National and local plans need to be put into action by the responsible identified owner for that plan as soon as possible to mitigate impact and risk to all.

4.2 **National and Strategic Team should be initiated only if:**

- One or more of the business-critical activities have been disrupted and there is no certainty about the timescales for recovery to be identified or achieved.
- Core services are lost to three or more individuals in any one location.
- One of our partners/stakeholders has initiated their BDRC response to which we need to provide support.

4.3 **Regional and Operational Team should be initiated if:**

- A serious incident occurs not meeting the threshold for the national team to be invoked.
- This refers to serious incidents at Level 3 accounted for in the Incident Management Policy and definitions / categories already established.
- Escalation of events can be communicated to SLT, and agreement reached if this event needs additional support. SLT leads will make the decision if it is suitable to invoke the National Strategic Team.

4.4 **Local Plans**

- The Operational Team should be initiated to manage and deal with all localised incidents escalating communications of events effectively.

5.0 Incident Reporting & Media Management

5.1 Any serious incident can create significant interest from the local and national media. Therefore, it is essential that only authorized staff can act as the nominated spokesperson for the Group.

5.2 In most cases the Chief Executive Officer/Communications Manager will be the only point of contact with the media and will inform the Chair or Vice Chair of the disaster/business continuity incident. In the absence of the Chief Executive Officer, the nominated strategic lead from SLT will have delegated authority to deal with media enquiries and authority to contact the Chair or Vice Chair.

5.3 The Chief Executive Officer may delegate responsibility to the Executive Director Housing and Support in regard to a business continuity event that involves:

- Media management; and
- Notifying the respective Chair of the Governing Body

5.4 The allocated SLT lead has delegated authority to contact the Regulator in relation to reporting the incident/emergency/disaster if it falls within the definition of a notifiable event.

5.5 Details of any BDRC event will be reported to Board and relevant committees in line with the Incident Management Policy. This report will focus on outcomes, recovery time and lessons learned to reduce and mitigate future such scenarios.

6.0 Review

6.1 The effectiveness of this policy will be monitored by the reviewing sub-Committee and or Chief Executive Officer.

6.2 This policy may be reviewed at any time at the request of either staff or management but will be reviewed every three years.

6.3 This policy will be shared with staff via Policy Hub and association newsletter.

7.0 Reference Documents

- Business Disaster Recovery and Continuity Plan
- Lone Working Policy
- Safeguarding Policy
- Incident Management Policy
- Business Plan
- Risk Register
- Epidemic and Pandemic Management Plan
- Managing Attendance and Sickness Procedure
- Accident/Incident and Near Miss Reporting & Investigation Policy and Procedure
- Incident Management Policy and Procedure (includes Serious Incidents)
- Fire Safety Management Policy and Procedure (includes Emergency Evacuation Planning) - under review as of October 2024
- Delegation of Financial Authority
- Probity Policy
- Data Protection Policy
- Cyber Security Policy
- Network Security Policy
- General Information Security Policy - under review as of October 2024
- Network Access and Data Security Policy - under review as of October 2024

Appendices*

1. Business Disaster Recovery and Continuity Plan - Proforma (includes Risk Assessment and Emergency Grab Bag Inventory)
2. Emergency Fire Procedure Template
3. Media Crisis Management Flowchart
4. Individual Site Management Details Proforma

**All appendices to be provided separately on Policy Hub.*