Reference Number: *UHB 559* **Version Number:** 1	**Date of Next Review:** *11/11/2028* **Previous Trust/LHB Reference Number:** *n/a*

Digital Disaster Recovery Policy

Policy Statement

To ensure the Health Board delivers its aims, objectives, responsibilities and legal requirements transparently and consistently, we will, in the event of a Business Continuity Event/Incident (BCP Incident) clearly define roles, responsibilities and ensure processes are in-place so that a coordinated response can be invoked to restore normal service. The Cardiff and Vale University Health Board (CAVUHB) Digital and Health Intelligence (D&HI) Disaster Recovery Policy has been established to ensure that this happens.

This policy specifically governs the restoration of digital infrastructure, systems, applications and hosted services following a disaster or major incident. It does not define or direct clinical business continuity arrangements, which remain the responsibility of the Chief Operating Officer (COO) and Clinical Boards. Clinical continuity is governed under the wider Business Continuity Policy and EPRR framework.

This policy provides technical recovery instructions for digital systems only. Clinical business continuity arrangements, including alternative methods of care delivery during digital outages, remain entirely under the governance of the COO and Clinical Boards. Both processes operate in parallel during major incidents and are coordinated via the EPRR structure.

Policy Commitment

The policy achieves this goal by;

a) Ensuring that roles and responsibilities are correctly mandated
b) Establishing a 'Disaster Recovery Team' to work within a clearly defined framework of remediation activity, enabling CAVUHB to recover from disaster scenarios
c) Defining Critical Infrastructure, Critical Platforms, and Mission Critical Services, including their respective owners and support requirements, to ensure their successful recovery can be achieved

Supporting Procedures and Written Control Documents

This Policy describes the following with regard to the Digital Disaster Recovery.

1. Scope

The CAVUHB D&HI Disaster Recovery Policy applies to all CAVUHB **Clinical Boards** and **Directorates**.
From a technology perspective, CAVUHB Disaster Recovery Policy applies to systems defined as **Critical Infrastructure and Platforms**, and **Information Assets**

For clarity, this policy applies solely to Digital & Health Intelligence functions and those

supporting the technical recovery of digital platforms. It does not describe or mandate clinical service continuity arrangements. Where a digital service failure affects clinical delivery, clinical operational teams retain responsibility for implementing alternative processes (e.g., paper workflows or contingency diagnostics).

This policy should be read in conjunction with wider organisational EPRR and business continuity documentation to avoid terminology duplication during major incidents.

2. Roles and Responsibilities

2.1 The Chief Executive

The Chief Executive is responsible for ensuring that the organisation can restore core services and critical infrastructure at predetermined levels in the event of a BCP event/incident. This includes providing the highest level of organisational commitment to the CAVUHB D&HI Disaster Recovery Policy and the availability of resources to support its implementation.

2.2 Chief Operating Officer (COO)

The COO is responsible for declaring a BCP Incident.

The COO's declaration of a BCP Incident does not automatically trigger clinical service failure procedures; instead, it triggers the technical digital recovery process described within this policy. Clinical boards continue to manage operational care delivery through established business continuity mechanisms.

*During office hours the COO will be responsible for declaring a BCP Incident, while out of hours this responsibility is delegated to the Executive On-call

2.3 Emergency Preparedness, Resilience and Response (EPRR)

The EPRR team are responsible for;

- Informing the SIRO that a BCP Incident has been declared.
- Assisting the Disaster Recovery Team by establishing and maintaining communications between the Disaster Recover Team, BCP Teams, and the COO for the duration of the BCP Incident response effort.

The Digital Disaster Recovery Policy is designed to integrate with CAVUHB's overarching EPRR arrangements. EPRR will ensure alignment between clinical and digital responses during major incidents, reducing duplication and ensuring clarity of command and control. This includes ensuring consistent use of terminology between digital and organisational incident commands.

*The EPRR team to do not operate an on-call service, so in the event of a BCP incident being declared outside of working hours, the Silver Tactical team would be engaged directly by the Disaster Recovery Team (see section 3.6 'Disaster Recovery Team')

2.4 Senior Information Risk Owner (SIRO)

The SIRO is responsible for;

- Providing authority for declaring a disaster and Invoking DR measures
- Ensuring a framework for DR remediation activity is in place
- Providing authority for the DR effort

2.5 CAVUHB Clinical Boards and Directorates

CAVUHB Clinical Boards and Directorates are responsible for;

- Ensuring the required assistance is provided to the SIRO during a BCP Incident for the duration of the DR effort, and for providing authority for their respective DR planning requirements detailed in the CAVUHB Disaster Recovery Policy.
- Invoking and managing required BCP and DR measures.

2.6 Disaster Recovery Team

The Disaster Recovery Team (see section 4 'The Disaster Recovery Team') are responsible for coordinating the DR effort. This may include (but is not limited to) the following;

- Damage Assessment
- Coordinating the recovery of critical Infrastructure and Platforms
- Executing system specific DR plans
- Coordinating the recovery of all effected Information Assets
- EPRR team engagement
- Coordinating any on-call requirements (including liaising with the tactical Silver team when required)

This team is responsible exclusively for restoring digital platforms, infrastructure, data availability and supporting applications. The DR Team does not assume responsibility for clinical service delivery, operational decision-making, or clinical continuity planning.

2.7 Digital Operations

The Digital Operations team are responsible for assisting the Disaster Recovery Team for the duration of the DR effort. This may include (but is not limited to) the following;

- Invoking and managing Incident Management procedures and triage (i.e. Incident

Management support)

- For areas of responsibility (see section 7 'Critical Infrastructure and Platforms'), managing the recovery of critical Infrastructure and platforms to full service
- Supporting the recovery of critical systems
- Supporting the recovery of Information Assets

The Digital Operations team are also responsible for maintaining accurate and up-to-date DR plans for areas of responsibility that are defined as 'critical' (see section 7 'Critical Infrastructure and Platforms'), ensuring they are regularly reviewed in accordance with agreed CAVUHB cyber security objectives.

During a major incident, Digital Operations will focus solely on restoring underlying digital systems and infrastructure. Clinical appropriateness, prioritisation of patient-facing services, and operational decisions remain with clinical leaders under business continuity governance.

2.8 Capital Estates and Facilities (CEF)

The CEF team are responsible for assisting the Disaster Recovery Team for the duration of the DR effort. Assistance requirements will vary depending on the declared disaster category (see section 6 'Disaster Definitions'), but may include managing the recovery of the Critical Infrastructure to full service for areas of responsibility (see section 7 'Critical Infrastructure and Platforms').
The CEF team are also responsible for maintaining accurate and up-to-date DR plans for areas of responsibility that are defined as 'critical' (see section 7 'Critical Infrastructure and Platforms'), ensuring they are regularly reviewed in accordance with agreed CAVUHB cyber security objectives.

2.9 Digital Healthcare Wales (DHCW)

DHCW are responsible for assisting the Disaster Recovery Team for the duration of the DR effort. Assistance requirements will vary depending on the declared disaster category (see section 6 'Disaster Definitions'), but may include managing the recovery of the Critical Infrastructure to full service for areas of responsibility (see section 7 'Critical Infrastructure and Platforms').
DHCW are also responsible for maintaining accurate and up-to-date DR plans for areas of responsibility that are defined as 'critical' (see section 7 'Critical Infrastructure and Platforms'), ensuring they are regularly reviewed in accordance with agreed CAVUHB cyber security objectives.

2.10 Service Leads

Service Leads are responsible for;

- Assisting the Disaster Recovery Team for the duration of the DR effort. Assistance requirements will vary depending on the declared disaster category (see section 6 'Disaster Definitions'), but may include providing resource to assist with the DR effort in restoring owned Digital Services to full operations.
- Maintaining accurate and up-to-date DR planning documentation for owned Digital Services.
- Categorising the criticality for owned Digital Services, adhering to the 'Service Categorisation Table' defined in section 4 of the Business Continuity Planning (BCP)

Guidance document

- Categorising owned Mission Critical Services, adhering to the definition detailed in section 8 'Mission Critical Systems' of the CAVUHB D&HI Disaster Recovery Policy

2.11 Cyber Security Team

The Cyber Security team are responsible for;

- Assisting the SIRO when making key decisions (e.g. declaring a disaster and invoking DR measures)
- Defining and maintaining the DR Policy and the Disaster Response Plan (see section 7 'Disaster Response Plan'), ensuring they are reviewed at least annually to provide both internal and external Security assurance

3. The Disaster Recovery Team

The Disaster Recovery Team will coordinate the DR effort and will be activated when the COO declares a BCP Incident, and the SIRO invokes DR measures. The team will evaluate the disaster and determine the steps required to restore the organisation to full service.
The Disaster Recovery Team consist of the following core members: -

- Head of Information Governance and Cyber Security
- Head of Digital Operations
- Cyber Security Team
- Digital Operations Team leads (TBC once disaster has been declared and support requirements known)

Additional members may be invited to join the Disaster Recovery Team to assist with the DR effort. This membership will depend on the declared disaster category (see section 5 'Disaster Definitions'), and may include (but is not limited to) the following;

- Team leaders or Senior Product specialists from affected services
- Heads of Department from affected services
- Service Leads

Digital Operations will support the DR effort by providing the Disaster Recovery Team with Incident Management and triage capabilities (see section 3 'Roles and Responsibilities').

4. Disaster Definitions

The SIRO is responsible for declaring a disaster. This decision will be made based on what

constitutes a disaster and how this is defined.
A disaster may be declared as a result of the COO declaring a BCP Incident. A BCP Incident may include (but is not limited to) any of the following

- Hardware and software failures (locally or nationally)
- Network and telecommunications loss
- Power outages
- Malware / ransomware
- Insider threats
- Vendor liquidation or cyber attack
- Inaccessible building (e.g. due to a local hazard)
- Equipment damage (e.g. due to fire, roof collapse)
- Natural disasters

For an event to be declared a disaster, it must be determined that mission essential services are either unavailable or materially affected by the event.

A disaster declaration for digital services does not indicate or imply a clinical system-wide failure. It indicates that digital systems supporting mission-critical services require immediate technical restoration. Clinical continuity arrangements operate in parallel and are not dependent on digital system availability.

5. The Disaster Response (DRes) Plan

The DRes plan is maintained by the Cyber Security Team (see section 4 'Roles and Responsibilities'), and will be made available to the Disaster Recovery Team. The Disaster Recovery Team will invoke the DRes plan once a disaster is declared by the SIRO. The DRes plan will consist of the following;

- Disaster Response Process
- Disaster Response Procedures

The DRes Process will define the series of tasks and activities required to restore the organisation to full service, and the DRes Procedures will support the process by detailing how the specific tasks or activities will be completed.

The DRes Process may consist of (but is not limited to) the following set of activities;

1. Determine what systems and processes have been affected by the disaster
2. Establish and maintain communications with the EPRR team, ensuring the DR effort is aligned to the on-going BCP Incident management process (e.g. BCP)
3. Communicate the disaster to the relevant stake-holders
4. Prioritise and structure the DR effort (see section 7 'Critical Infrastructure and Platforms' and section 8 'Mission Critical systems')
5. Invoke any required out-of-hours support arrangements
6. Activate DR plans in prioritised order
7. Determine regulatory reporting requirements (see section 10 'NIS Incident Reporting')

8. Ensure that all decisions made abide by the Disaster Recovery Policy and all relevant policies set by CAVUHB
9. Notify the relevant parties once the disaster is over and normal service has been restored
10. Provide a report to the SIRO summarising the activities undertaken during the disaster and rationale for key decisions

6. Critical Infrastructure and Platforms

The following Infrastructure and Platform services have been defined as critical by the CAVUHB D&HI Disaster Recovery Policy;

- Local Area Network (LAN) Infrastructure
- Wide Area Network (WAN) Infrastructure
- Domain Name System (DNS)
- Power Infrastructure
- Telecommunications Infrastructure
- Authentication Services (e.g. Active Directory)
- Data Centre Services (servers, storage and core devices)

Critical Infrastructure and platforms must be returned to full operations before any Critical Services can be restored, so must be a priority for DR recovery measures and assigned the highest priority 'action' in the Dres plan.

The following support areas have been defined as owners for their respective Infrastructure and Platform services by the Disaster Recovery Policy, and are therefore responsible for DR planning and returning them the full operations in the event of a Disaster (see section 3 'Roles and Responsibilities');

1. **Digital Operations**
   - Local Area Network (LAN) Infrastructure
   - Telecommunications Infrastructure
   - Domain Name System (DNS)
   - Data Centre Service (servers, storage and core devices)

2. **Capital Estates and Facilities (CEF)**
   - Power Infrastructure

3. **Digital Healthcare Wales (DHCW)**
   - Wide Area Network (WAN) Infrastructure
   - Authentication Services (i.e. Active Directory)
   - Cyber
   - M365 tenant

These components are prioritised for restoration because they underpin mission critical digital services. Their restoration does not replace clinical decision-making but enables the reinstatement of digital tools used by clinical teams.

7. Mission Critical Services

The CAVUHB D&HI Disaster Recovery Policy defines Mission Critical Services as;
"Any information system or asset whose failure or compromise would significantly impact the organization's ability to achieve its objectives, violate legal or regulatory requirements, or cause substantial harm to patient care"

Any Service that can be categorised as 'Mission Critical' must be restored to full operations once Critical Infrastructure and Platforms have been restored. This priority must be reflected by the DRes plan.

'Mission Critical' Service Leads must maintain compliance with the responsibilities defined in sub-section 3.10 'Service Leads' of the CAVUHB Disaster Recovery Policy.

Mission Critical Services refer to digital systems only. Determination of clinical mission-criticality for patient services remains the responsibility of the COO and Clinical Boards under Business Continuity governance.

8. Appendix

NIS Incident Reporting

The Network and Information Systems (NIS) Regulations require Operators of Essential Services (OES) to notify the Competent Authority (Welsh Government via the Cyber Resilience Unit) of incidents without undue delay and no later than 72 hours after the OES is aware that a notifiable incident has occurred, and in line with the National Cyber Security Centre's Incident Management Guidance.

Thresholds for Incident Reporting for Operators of Essential Services (OES)
Any incidents that have an adverse effect on the confidentiality, integrity or availability of the health board's critical systems need to be reported to Welsh Government **if the incident meets specific thresholds**.
An incident would be NIS reportable from 'Catastrophic' to 'Moderate' only if the **resolution time** could not be met, **or the other impact descriptions** were realised as a result of the event.

Impact	Report Incident	Description

Catastrophic	Yes	Incidents which cause extensive business and/or clinical risk and prevent the user from providing a normal service. These would typically be incidents which: • cause unavailability of the entire service to the end user for 4+ hours • cause incorrect processing of data or errors in a key system function • cause extensive business and/or high clinical risk
Significant	Yes	Incidents which cause significant business and/or clinical risk and limit the ability of the user to provide a normal service. These would typically be incidents which: • cause unavailability of a key module or key system function for 4+ hours • cause incorrect processing of data or errors in a system function • cause a significant clinical risk
Moderate	Yes	Incidents which cause limited business and/or clinical risk and limit the ability of the user to provide a normal service. These would typically be incidents which: • cause unavailability of a non-key module or system function of a service for 8+ hours • cause a moderate clinical risk
Minor	No	Incidents which cause minor or negligible business and/or clinical risk and affect non-key system functions. These would typically be incidents which: • do not cause disruption of services; and • leave all system functions available but restrict performance, causing inconvenience but not disruption of service

Where a reportable cyber or digital incident affects clinical delivery, the Digital & Health Intelligence team will coordinate technical reporting requirements, while operational impact reporting remains the responsibility of clinical leadership.

Other supporting documents are:

List all documents the reader needs to be aware of alongside / in support of this document

- *Business Continuity Policy*

Scope

This policy applies to all of our staff in all locations including those with honorary contracts.	
Equality Impact Assessment	An Equality Impact Assessment (EqIA) has not been completed because this policy has been written to support the Business Continuity Policy, for which the EqIA found no impact.

Health Impact Assessment	A Health Impact Assessment (HIA) is not required for this policy.
Policy Approved by	Digital & Infrastructure Committee
Group with authority to approve procedures written to explain how this policy will be implemented	For example: Health System Management Board
Accountable Executive or Clinical Board Director	Director of Digital & Health Intelligence

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Governance Directorate.

Summary of reviews/amendments

Version Number	Date Review Approved	Date Published	Summary of Amendments
1	11/11/2025	20/01/2026	*New document.*