Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit

IGDC • DHCW

Expectations Guidance Document

5-Business Continuity

Introduction

This guidance will provide basic information on what will be required from Organisation Administrators and Users to work through and complete the Business Continuity section of the Welsh Information Governance Toolkit (WIGTK).

In the event of a major disruption to services such as cyber-attacks, floods, and supply failures, the organisation needs to have a plan in place to be able to continue to function with as little disruption as possible, where vital business processes can still be carried out. Having documented business continuity plans and procedures assists with this and enables staff to know how to carry out their roles in these types of scenarios.

Business Continuity Plans (BCPs) represent how organisations predict, assess, and counteract threats and risks that may lead to events that seriously disrupt all or part of their business functions. They determine what the organisation can do if certain scenarios happen, and how the organisation would systematically adapt to and recover from these events.

GMPs may require support from their appropriate commissioning Health Board to put appropriate plans and procedures in place.

Minimum Expectations

Plans and responsibility

The organisation should include information and cyber security content in its BCP. Or alternatively, have a separate IT disaster recovery plan to assess any potential risks to data and mitigate where possible.

Whichever route the organisation chooses, data security should be included in any plan, even those not related to cyber security incidents.

The ICO expects the organisation have plans to deal with serious disruption, with key systems, applications and data backed up to protect against loss of personal data.

Your organisation may also have a Disaster Recovery Plan to manage disasters, which identifies records that are critical to the continued functioning of the organisation.

All continuity plans should have privacy-by-design baked in, as the backup process could introduce other risks.

Your organisation should have appointed an individual or team with the responsibility for the information and cyber security business continuity. This may include having Job Descriptions assigning responsibility, organisational charts, or named individuals on BCP.

The requirements for Business continuity, disaster recovery and back-ups are set out within the Information and Cyber Security section of the ICO's Accountability Framework.

Testing the plan
It is extremely important that BCPs and disaster recovery plans are regularly tested, to test their effectiveness. It is recommended that these tests are actioned annually and whenever the organisation has a significant change in suppliers, systems or processes.

Tabletop exercises or simulations that include a cyber-scenario (such as a hacking) should be used to test that the BCP is fit for purpose and key staff understand their roles and what is expected of them in those scenarios.

This includes regularly testing back-ups and recovery processes to ensure they remain fit for purpose.

Emergency contacts
Emergency contact details should be kept securely, in hardcopy, and kept up to date.

Contacts should include names, phone numbers as well as e-mail addresses to ensure resilience should one form of communication be impacted by the event.

Contact details should be kept in hard copy form in case of system failure, it is especially important to review these regularly to check the accuracy.

Staff Awareness
All staff should be made aware of potential implications the BCP has on their role and how they can access the plan if required. Where practicable, staff should be involved in testing exercises, to further increase their awareness of the BCP and what is expected of them in case of emergency.

Examples of ways that staff can be made aware of the BCP or any changes to it are regular communications or documents showing relevant staff have read and understood the organisations BCP.

Data Backups – Not applicable to GPs
You should take back-up copies of electronic information, software, and systems, and ideally store them off-site for ease of access in case of any issues accessing internal systems.

You should be able to evidence that the backups, testing, and review processes are effective and carried out regularly. It is recommended that these are actioned annually. The frequency of backups should reflect the sensitivity and importance of the data, and organisations should identify any critical systems and information assets.

Exceeded Expectations

This section is not required to be completed; however, it will help to further demonstrate your compliance and provide assurance.

These questions build on those you will have answered in the minimum expectations section; however, they are slightly more in depth.

Reviewing the plan

Given the importance of these documents, it is essential that they are reviewed regularly and remain accurate, as it could have huge impact on service delivery in an emergency if the details within the plan are incorrect.

Evidence of this could include minutes of meeting showing review and updates or a log on the document that shows last review date and what changes were made.

Approval

The board, or highest senior management level, has overall responsibility for data protection and information governance. Therefore, the BCP should be approved by this forum before it is signed off, for example Practice Management Team, Senior Partners, or Board.