A logo for a company

Description automatically generated

Business continuity plan template for data and cyber security and how to test your plan

Published 28 January 2021 - Version 1

This document sets out a template for a business continuity plan to cover data and cyber security for your organisation and makes suggestions as to how you can test your plan to see if it will work in practice.

Data and cyber security plans should be added to your existing Business Continuity Plan. This document only covers electronic data as we presume that your existing Business Continuity Plan will cover risks to paper-based records e.g. fire, flood, loss of records etc.

The [Care Provider Alliance has produced additional guidance on business continuity planning](https://careprovideralliance.org.uk/business-continuity) including:

* A Business Continuity Planning Template
* Business Continuity Planning Guidance
* Fuel Supplies and Transport: Business Continuity Guidance
* Non-medical consumables goods and service: Business Continuity Guidance
* Medicines and medical devices: Business Continuity Guidance.

Completion of this template will help you provide evidence for the following [Data Security and Protection Toolkit](https://www.dsptoolkit.nhs.uk/) question:

*7.1.2 – Does your organisation have a business continuity plan that covers data and cyber security?*

# Introduction

This document sets out:

* What **digital systems and devices** the organisation currently has in place. This includes identification of ‘critical’ systems and devices
* **Business continuity scenarios**.  The organisation considers 6 different scenarios in terms of threats and for each a continuity plan is provided:
  + Office unavailability – e.g. through fire/flood
  + Phoneline / broadband failure
  + Power cut
  + Broken computer
  + If you were hacked
  + If your supplier’s system failed e.g. care planning system
* **Business continuity plan testing**. How we test our plans, and record what tests have we carried out and when, and any remedial action taken.

This plan is reviewed and updated on an annual basis, and when any critical systems are changed or new systems introduced.  Reviews are part of the annual tasks around data and cyber security as set out in our Data security policy/plan stored here: [add link].

# When was this plan last reviewed and tested? Who has seen it?

|  |  |  |
| --- | --- | --- |
| Date of review | Document signed off by | Document distributed to (e.g. registered manager, management team, directors, trustees) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# What digital systems and devices does the organisation currently have in place?

## Digital systems

Complete one row below for each of the organisation’s digital systems.  Examples of systems that you might have are as follows:  Email (e.g. NHSMail, and/or another email system); care planning; HR/Staffing system; payroll; document storage (e.g. Dropbox, Google drive); electronic MAR charts; accounts and finance system; office phone system; CCTV software

|  |  |  |  |
| --- | --- | --- | --- |
| Digital systems | Rate the impact of these systems failing in terms of severity (1 – 10) 1 being low, 10 being high | Can you use an alternative method e.g. paper – based alternative? If so where is this stored? | Date Completed |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Devices

Complete one row below for each of the organisation’s devices.  Examples of devices that you might have include: servers, desktop computers, laptops, tablets, smartphones, memory sticks.

Include any devices that are personal that are used for work purposes, e.g. if the owner uses their personal smartphone to access company emails, then this should be included in this list.

|  |  |  |
| --- | --- | --- |
| Device | Rate the impact of these systems becoming broken/lost/stolen in terms of severity (1 – 10) 1 being low, 10 being high | Date Completed |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Critical systems and devices

Complete one row below for any system or device rated over a 5 in severity (in 3.1 and 3.2 above) – these are our ‘critical systems’.

|  |  |  |  |
| --- | --- | --- | --- |
| Critical systems | Provider / Contact details | For critical systems:  Does the supplier have their own business continuity plan in place? Where can this be found? | Date Completed |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Business continuity: scenarios

## Scenario 1 – Office unavailability

Consider how you would access the information and systems that you need to run the business, should one or more offices become unavailable.  For example, if there is a fire or flood, and office phones, computers and servers are irretrievably lost/unavailable.

|  |  |
| --- | --- |
| Consider | Continuity plan |
| How will we access our systems and data e.g.   * what other computers can we use * where will we work from * can we get our data back from our backups * how will we access the internet (e.g. for email and other online systems) |  |
| If this happens, who needs to do what, and by when |  |
| Who needs to be told and how will we tell them | e.g. colleagues, other organisations, families |
| What needs to be put in place so that our plan will work, who will do this and by when |  |

## Scenario 2 - Phoneline / broadband failure

Consider what would happen if your phone lines and broadband were to fail.  For example, would you be able to access care plans? Would you be able to access the telephone numbers for service user’s families for example? Would you be able to direct staff to where they need to be to provide care to service users?

|  |  |
| --- | --- |
| Consider | Continuity plan |
| What external telephone numbers are critical to running the business and how will we know what numbers these are? |  |
| What will we use to make phone calls? |  |
| How will we connect to the internet (e.g. for email, and any other online critical systems) | *e.g. by using a ‘dongle’ or mobile phone wifi hotspot or home broadband* |
| If this happens, who needs to do what, and by when |  |
| Who needs to be told and how will we tell them | *e.g. colleagues, other organisations, families* |
| What needs to be put in place so that our plan will work, who will do this and by when |  |

## Scenario 3 - What would happen in the event of a power outage?

Consider how you would access the information and systems that you need to run the business, should you experience an extended power cut.

If you have a laptop this would last for a period of time using its battery power.  You could consider investing in an Uninterruptible Power Supply (UPS) system that will provide power, so your plugged-in devices remain powered (for e.g. a couple of hours) despite a black out.

|  |  |
| --- | --- |
| Consider | Continuity plan |
| How will we access our systems and data e.g.   * where will we work from * what computers can we use * how will we access the internet (e.g. for email and other online systems) * For critical systems that are not online, how can we access what we need? |  |
| If this happens, who needs to do what, and by when |  |
| Who needs to be told and how will we tell them | *e.g. colleagues, other organisations, families* |
| What needs to be put in place so that our plan will work, who will do this and by when |  |

## Scenario 4 - What would happen if a device failed? What would happen if a device became lost or stolen?

Consider the devices you identified in 3.2 above; what action would be needed if one of these devices became broken, or was lost or stolen?

Is your service reliant on one main computer or laptop or do you have other devices that you could use if the computer/laptop stopped working?

Laptops, tablets and smartphones are particularly vulnerable to becoming lost or stolen. Do you protect them to prevent unauthorised access?  E.g. is there a pin, fingerprint or facial scan? Is there an app set up to track the location of a lost/ stolen smartphone, and ‘wipe’ its contents remotely?

To make laptops and tablets especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people) – you then need a ‘pin’ or password to start up the device.  Or, you can use ‘two factor authentication’ – a security process which requires more than a single password, for example a fingerprint or facial scan, or a security token (e.g. a smart card or key fob which displays a number which you then put into the device to access it).  You must also have an operating system password (something different to the original password the device came with) to access the software e.g. email/Word.

|  |  |
| --- | --- |
| Consider | Continuity plan |
| How will we access our systems and data e.g.   * what other device/s can we use * if necessary, can we get our data back from our backups * how will we prevent our data getting into the wrong hands |  |
| If this happens, who needs to do what, and by when | *If a device is lost or stolen then you would need to follow your breach reporting system.  For a data security breach incident reporting form see: https://www.digitalsocialcare.co.uk/resource/data-security-breach-incident-reporting-form-template/* |
| Who needs to be told and how will we tell them | *e.g. colleagues, other organisations, families* |
| What needs to be put in place so that our plan will work, who will do this and by when | *For broken equipment:*  *e.g. set up a spare computer ready to use*  *e.g. make sure information can be restored from our (regular) backups*    *For lost or stolen:*  *e.g. make sure our devices are difficult to get into, by using encryption or two factor authentication; using strong passwords / pins; fingerprint or facial recognition*  *e.g. make sure that lost or stolen devices can be tracked and ‘wiped’ remotely*    *Bring your own device*  *Make sure that you have a Bring Your Own Device policy to cover arrangements for personal devices (e.g. such as a smartphone)* |

## Scenario 5 - What would you do if you were hacked?

If you are hacked then you’ll need to act quickly and get the right support – it’s therefore important to have a robust plan in place.  The best way to avoid being hacked is to follow good practice in terms of technical approaches but also importantly by making sure staff have the right training.

Do you protect your devices from malware?  Malware is malicious software (such as viruses) designed to cause damage – for example deleting all your data or blocking access to it until a sum of money is paid.

Out of date operating systems (e.g. versions of Windows or MacOS that are no longer supported by the manufacturer, or supported versions of Windows or MacOS which are not subject to regular updates) are vulnerable to this type of attack. Do you keep operating systems for your computers and smartphones updated or ‘patched’?

Antivirus software helps protect your computers/laptops – is this in place?  A firewall (which can be software) blocks unauthorised access from outside of your organisation – do you have one of these?  Do you avoid unsecure or public wifi?

In terms of staff training, all staff should be made aware of what to look out for as part of induction training and then provided with reminders at least annually and/or highlighted in other ways such as on agenda of regular meetings or in supervision. See [Staff training guidance June 2020](https://www.digitalcarehub.co.uk/resource/staff-training-guidance-june-2020/).

|  |  |
| --- | --- |
| Consider | Continuity plan |
| If this happens, who needs to do what, and by when | **Contact Action Fraud**  Action Fraud is the UK’s national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cyber crime. You [can report fraud or cyber crime using their online reporting service any time of the day or night](https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime); the service enables you to both report a fraud and find help and support. You can talk to their fraud and cybercrime specialists by calling 0300 123 2040    **Follow the breach reporting procedure**  For a data security breach incident reporting form see: https://www.digitalsocialcare.co.uk/resource/data-security-breach-incident-reporting-form-template/    **Change passwords**  Passwords should only ever be changed if they’ve been compromised, this is an instance where they would need to be changed    **Obtain technical advice and support**  IT Support can help with repairing computers if this is needed    **Restore backups**  If necessary, as a way of retrieving your information |
| Who needs to be told and how will we tell them | e.g. colleagues |
| What needs to be put in place so that our plan will work, who will do this and by when |  |
| What prevention measures do we have in place in terms of our technical approaches? | Keep operating systems and software up to date for all devices  Use anti-virus software on computers and laptops  Implement a firewall for your offices’ internet connections  Avoid unsecure or public Wi-Fi |
| What prevention measures do we have in place in terms of staff training? | Staff awareness training – as part of induction  Reminders and/or retraining annually |

## Scenario 6 - What would happen if a supplier had a fault? i.e. the care planning system won’t work and it’s the supplier’s fault?

Consider how you would access the information and systems that you need to run the business, should a critical system provided by an external supplier stops working, where this is the supplier’s fault.

Here you will need to consider sector specific software, such as care planning systems, rota systems, electronic MAR sheets etc.  Global systems such as Google, Dropbox or Microsoft fail sufficiently rarely that continuity plans are not typically necessary.

What if the system was down for an extended period? What paper or alternative systems (identified in 3.1 above) would you be able to put into place?

You should refer to your critical systems and the provider’s contingency plans identified in 3.3 above.

|  |  |
| --- | --- |
| Consider | Continuity plan |
| What critical aspects of our business will be affected? |  |
| How will we access the information that we need? | e.g. through restoring our data from backups  e.g. putting a temporary paper or spreadsheet system in place |
| If this happens, who needs to do what, and by when | e.g. who to contact at the supplier organisation |
| Who needs to be told and how will we tell them | e.g. colleagues |
| What needs to be put in place so that our plan will work, who will do this and by when | e.g. local daily backups which could then be restored  e.g. weekly paper printout of the rota |

# Business continuity plan testing

It is good practice to ensure that our business continuity plans work well.  This section details the activities we undertake annually to test our business continuity plan for those devices and digital systems considered critical and for ‘typical’ scenarios, and provides evidence that we have done this for this year. The tests that we undertake are designed to help secure staff engagement through upbeat and interesting exercises, to support learning in the area of business continuity.

## Scenario 1 tests – Office unavailability

|  |  |
| --- | --- |
| Test | Office unavailable    *Lock the door of one office to simulate the office becoming unavailable.  Go through the steps in your plan in 4.1 above to see if it works.* |
| Details including who carried out the test, when, and who was involved |  |
| Test results |  |
| Remedial actions? |  |
| Date test completed |  |

## Scenario 2 tests - Phoneline / broadband failure

|  |  |
| --- | --- |
| Test | Phoneline/broadband failure    *In the office, unplug the telephones, and for computers, laptops and smartphones, switch off the Wi-Fi on each device (or unplug the cable) so that internet access is not possible.*  *Go through the steps in your plan in 4.2 above to see if it works.* |
| Details including who carried out the test, when, and who was involved |  |
| Test results |  |
| Remedial actions? |  |
| Date test completed |  |

## Scenario 3 tests – Power outage

|  |  |
| --- | --- |
| Test | Power outage    *Unplug relevant devices in one office to simulate a power cut, or you can replicate this by putting paper in front of screens and turning the lights off.*  *Go through the steps in your plan in 4.3 above to see if it works.* |
| Details including who carried out the test, when, and who was involved |  |
| Test results |  |
| Remedial actions? |  |
| Date test completed |  |

## Scenario 4 tests – Broken or lost/stolen devices

|  |  |
| --- | --- |
| Test | Broken laptop    *Temporarily ‘hide’ a company laptop.*  *Go through the steps in your plan in 4.4 above to see if it works.* |
| Details including who carried out the test, when, and who was involved |  |
| Test results |  |
| Remedial actions? |  |
| Date test completed |  |

|  |  |
| --- | --- |
| Test | Stolen smartphone    *Temporarily ‘hide’ a personal smartphone.*  *Go through the steps in your plan in 4.4 above to see if it works.* |
| Details including who carried out the test, when, and who was involved |  |
| Test results |  |
| Remedial actions? |  |
| Date test completed |  |

## Scenario 5 tests – Ransomware attack

|  |  |
| --- | --- |
| Test | Ransomware attack    *To undertake this test attach the slideshow below to an email and send this to staff, following the instructions below.* |
| Details including who carried out the test, when, and who was involved |  |
| Test results |  |
| Remedial actions? |  |
| Date test completed |  |

**Powerpoint slide show – example of wording**

*You can send this PowerPoint slideshow as an attachment to an email.  For the email use wording that could have been made up by someone outside of your organisation, for example you could say something like “Hello, could you just give this a quick check for me please?” to see if the recipient opens the attachment.*

*When the recipient opens the slideshow this opens the presentation immediately to recreate the effect of a ransomware ‘taking over’ the recipients screen:*

** Double click - This version opens up automatically

 (Standard PowerPoint version, this can be edited)

*Talk through the with the member of staff the steps that they would then need to take as a result of suffering from a ransomware attack.  Talk though ways to spot suspicious emails and what to do about them. For more information see* [advice from the National Cyber Security Centre](https://www.ncsc.gov.uk/collection/phishing-scams).

## Scenario 6 tests – Supplier fault

|  |  |
| --- | --- |
| Test | Supplier fault  *Choose one critical system which is supplied by an external supplier.  Log out of the system to simulate the system being unavailable.*  *Go through the steps in your plan in 4.6 above to see if it works.* |
| Details including who carried out the test, when, and who was involved |  |
| Test results |  |
| Remedial actions? |  |
| Date test completed |  |