[14] Business Impact Analysis Document - Template

Risk Assessment Descriptors: Use the descriptors below to assess the LIKELIHOOD of a risk occurring					
Score	5	4	3	2	1
Descriptor	Probable	Possible	Unlikely	Rare	Negligible
Likelihood of occurrence	More likely to occur than not	Reasonable chance of occurring	Unlikely to occur	Will only occur in rare circumstances	Will only occur in exceptional circumstances
	greater than 50% chance	between 50% and 5%	between 5% and 0.5%	between 0.5% and 0.05%	between 0.05% and 0.005%
	greater than 1 in 2 chance	1 in 20 chance	1 in 200 chance	1 in 2000 chance	1 in 20,000 chance
Risk Impact: Use the descriptors below to assess the IMPACT severity if a risk occurs					
Score	5	4	3	2	1
Descriptor	Catastrophic	Major	Moderate	Minor	Insignificant
Severity of impact	Permanent loss of core service or facility	Sustained loss of service which has serious impact on delivery of care.	Some disruption in service & unacceptable impact on care. Non-permanent loss of ability to provide a service	Short term disruption to service with minor impact on care	Interruption in a service which does not impact on the delivery of care or the ability to continue to provide a service

Record the likelihood and impact of potential hazards and/or threats together with the recovery time-frame options.					
			Option 1	Option 2	Option 3
Hazard or threat	Likelihood Score	Impact Score	(2 hours)	(24 hours or more)	(5 days or more)
Loss of main premises					
Loss of computer systems/ essential data					
Loss of telephone system					
Loss of essential supplies					
Loss of health records					
Incapacity of lead professional					
Incapacity of support staff					
Loss of electricity supply					
Loss of gas supply/ heating					
Loss of water supply					
Loss of security systems					

[15] Emergency & Business Continuity Plan – Exemplar Text

[The following text, or similar, should be inserted into your Business Continuity Plan. It details procedures relating to Information Governance. Please note that this plan assumes that you are using paperless working as far as possible and that you might have digital care planning software, if this is not the case then not all of the following would need to be included in your plan. Your IT supplier or support will be able to help with this.]

Business Continuity Plan

In the instance that there is a loss of the main premises, **[insert name here]** will need to contact the ICT supplier regarding data restoration. The ICT supplier is **[insert supplier name here]** and they can be contacted **[insert contact details here]**.

1. Information Assets

1.1. **[Insert organisation name here]** maintains, separately to this document, an Information Asset Register which contains details of all information assets pertinent to the business. This register is stored **[insert hard copy location and location on computer system of Information Asset Register].**

2. Loss of computer system/essential data

2.1. The supplier must be notified immediately if either computer hardware or the core software are lost **[insert contact details]**. The equipment and software will ultimately be replaced, but short term, it has been agreed that the following will be made available at **[insert name of temporary accommodation]**:

i. PC's and printers to enable business continuity;

ii. Access to a photocopier;

iii. Access to a fax machine;

iv. The facility to scan and attach post [this would not be classed as urgent to ensure business continuity in the short term].

2.2. Computer backups are made **[insert how often. If applicable, you may wish to state which files are backed up].** Any information assets selected for backup are encrypted during the backup process using **[insert encryption type here]**. There is no transmission of information assets in an unencrypted form. The key for the encryption is held in the following places: **[insert location]**

2.3. The transmission of the encrypted data files is done using an authenticated and IP address restricted FTP server. All data in transit is encrypted prior to transmission and all data at rest is stored in an encrypted format. **[Insert how long you retain backups for here. This sounds complicated, but your ICT supplier or support should be able to help and provide advice on what would be appropriate for your organisation.]**

2.4. The Information Asset Register contains information on mobile devices with secure remote access to the care planning system. These may be available to facilitate immediate access if the server is unaffected. **[if your organisation does not use digital care planning software then this will not be relevant for you.]**

3. <u>Recording data</u>

3.1. If there is a failure in the ICT system or any standalone computer, the staff will revert to a paper backup system to capture that important data so this can be recorded on the system retrospectively. Templates for recording information when the system is unavailable can be found **[insert location]**.

3.2. Once information is captured on the paper templates these are kept securely **[insert location here]** until they can be entered onto the computer

system. Once they have been entered and validated the paper documents are securely disposed of. **[If you do not run a paperless system, then your usual storage procedures should be followed. If you do not revert to a paper system in case of a failure in the ICT system, then detail your procedures here instead.]**

4. Loss of care records

4.1. Paper care records are stored in cabinets in **[insert location]**, and are protected from any untoward event by **[insert your organisation's procedures here]**.

4.2. **[insert number]**% are summarised onto the care planning system and could be reconstructed from data held on the computer system if necessary.