**BUSINESS CONTINUITY PLAN TEMPLATE**

This template is designed to provide the outline for a simple plan that identifies key people, activities and documents, vulnerabilities and recovery time tolerances on your unit’s activities as they relate to the School’s business, and how to deal with the consequences of a non-specific incident.

It can be split roughly into three parts. The first part (items 1-9 on the contents list) deals with information gathering, the second part (items 10-12 on the contents list) provides templates that you may wish to use or adapt when an incident actually happens and the third part (item 13 on the contents list) is the lessons learnt / incident log.

You may wish to add to this template, or there may be sections which are not relevant to you. It is not an exhaustive guide, but a tool that can be adapted to reflect the work that your unit does that is critical to the School’s business and to assist you in your business continuity planning. There may be other information you wish to capture, or you may wish to use alternative methods of displaying the information in your plan. There is nothing to stop you adding sections, or taking out sections that do not apply to you or are not useful to you.

It is impossible to plan for every situation or scenario, and business continuity is about planning how you would respond to the consequences of an incident that affects the School’s business, not necessarily identifying the incident itself, in a way that allows your area to resume business activities critical to the School as quickly as possible. To do this you need an understanding of what is critical to your area and how you would recover it if necessary.

Things to consider:

* What critical activities do you undertake for the School? E.g. payroll, exams, teaching etc.
* What times of year are critical for you?
* Do you need to share specialist knowledge more widely in your area?
* Are there areas where you are particularly vulnerable?
* Who do you need to contact in an emergency?
* How would you contact people in an emergency?
* Have you considered what you would do in some common scenarios? For instance, do you know what to do if:
  + You cannot access your offices or teaching space for any reason;
  + Staff/students cannot travel into the School;
  + You cannot access your IT dependent systems;
  + There is a threat to your area’s reputation;
  + What happens if there is an incident at your most business critical time of the year;
  + What happens if you have insufficient staff to undertake business critical activities, or you are short staffed at a business critical time of year?
  + You lose business critical or confidential data, e.g. staff records, exam scripts, contracts, loan agreements etc?

**<UNIT NAME>**

**Business Continuity Plan**

*By <NAME OF AUTHOR/OWNER>*

*Version no: Version Date:*

**CONTENTS:**

1. **Purpose, scope, objectives, assumptions of plans**
2. **Revisions to the plan: control log**
3. **Contacts**
4. **Business critical data (includes confidential data)**
5. **Business critical data log**
6. **Alternative accommodation arrangements**
7. **Business critical activities log**
8. **Business critical activities calendar**
9. **Business critical systems log**
10. **Example of an initial assessment form following an incident**
11. **Checklist of steps to take in the event of an incident**
12. **Example of a check list for an activity or task**
13. **Lessons learnt / incident log**

**Distribution:**

|  |  |
| --- | --- |
| **Copies held by:** | **Location of copies:** |
|  |  |
|  |  |
|  |  |

***Purpose***

The purpose of this business continuity plan is to prepare the <UNIT> in the event of disruption to services and business critical activities that it undertakes for the School, caused by factors beyond its control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.

The plan identifies business critical activities and vulnerabilities and recommends measures to recover business critical activities and prevent extended disruption to the School’s business as undertaken by the <UNIT>.

The plan identifies recovery tolerances for business critical activities.

## Scope

The scope of this plan is limited to <describe>. This is a localised business continuity plan designed to help the <UNIT> protect and restore the functions that it contributes to the School’s business, not a daily problem resolution procedures document. It is not a School wide problem resolution procedure, nor should it be used to replace the School’s MIIRP procedure or over-ride instructions from the School’s Gold/Silver/Bronze teams in the event of an emergency.

## Plan objectives

* Serves as a guide for those responsible for recovery of the School’s business critical activities within the <UNIT>.
* References and points to the location of critical data.
* Details the procedures and resources needed by the <UNIT> to assist in recovery.
* Identifies those people and groups, internal and external, who must be notified in the event of an incident within the <UNIT>.
* Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
* Identifies alternate sources for supplies, resources and locations.
* Documents storage, safeguarding and retrieval procedures for vital records.

## Assumptions

* Key people (designated departmental/divisional leaders, business continuity representatives etc) will be available following an incident within the <UNIT>.
* National and School wide incidents are beyond the scope of this plan.
* This document and all vital records (or copies thereof) are stored in a **secure** off-site location and are accessible immediately following the incident to key people.
* That the first function of the plan is to restore those activities critical to the business of the School.
* *OPTIONAL: Each part of the <UNIT> will have its own plan consisting of unique recovery procedures, critical resource information and procedures if not already covered by this plan.*

## Team member responsibilities

* Each key team member will designate a deputy for when they are absent.
* All of the identified key people should keep an updated copy of the contacts list at home, and at work, with their colleagues’ work, home, and cell phone numbers.
* All key people should keep this plan for reference at home in case the incident happens after normal work hours.
* All key people should familiarize themselves with the contents of this plan.
* All key people should be willing to be contacted after normal working hours.

**Revisions to the Plan: Control Log**

|  |  |  |
| --- | --- | --- |
| **Date** | **Summary of changes made to the plan** | **Changes made by (Name)** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**CONTACTS**

The key people/emergency contacts in your unit should be able to contact each other and their colleagues as necessary in the event of an incident or emergency.

The principles of the **Data Protection Act** make it essential that an individual’s personal information can be used only with their express permission and only for a pre-defined purpose.

When adding contact details to this plan, you must be sure that the individual concerned has been informed to whom these details will be circulated, and for what purpose.  If that purpose changes or the circulation list changes you should let them know.

It is recommended that the contact person’s agreement be gained in writing/by email so that everyone is clear about the circumstances under which they may be contacted or their details circulated.

A column has been provided to outline the contact’s role/responsibilities in the event of an incident – this is optional.

A key person/emergency contact should be willing to provide ways to contact them when they are off campus and offline, i.e. a mobile number, and to be contacted out of hours.

**Emergency notification:**

*(who HAS to know, e.g. head of department/division, departmental manager, business continuity Rep)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Address** | **Home & Work** | **Mobile phone** | **Role event of an incident** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Key People:**

*(Key colleagues who have a role to play should an incident occur)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Address** | **Home & Work** | **Mobile phone** | **Role in event of an incident** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Other relevant internal contacts / recovery team contacts:**

*(who needs to know or who can provide help or more information, e.g. a departmental / divisional administrator, key academics, IT, Estates or Security contacts*)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Address** | **Home or work** | **Mobile phone** | **Role in event of an incident** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**External contacts:**

***(are there any external agencies that might need to be contacted? E.g. neighbouring organisations, contractors etc)***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Address** | **Home or work** | **Mobile phone** | **Role in event of an incident** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

BUSINESS CRITICAL DATA

Guidance on Electronic data: <http://www2.lse.ac.uk/intranet/LSEServices/IMT/infosec/home.aspx>

Guidance on Physical data: <http://www2.lse.ac.uk/intranet/LSEServices/legalandCompliance/recordsManagement/Home.aspx> -

**Data in the School:**

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of LSE. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for LSE to recover.

**Confidential Data:**

Any security breach of confidential data will be handled in accordance with all relevant School policies. Any security breach which also involves data classified as Confidential under the Data Protection Act may result in legal action being taken against the School and disciplinary action against an individual or individuals.

**Classification of Data:**

Not all critical data is confidential data. You can find the School’s data classification policy here: <http://www2.lse.ac.uk/intranet/LSEServices/IMT/about/policies/documents/infoSecClassification.pdf>

If you are unsure or require further information please see the websites above or contact the School’s Information Security Manager/Records Manager.

**Electronic Use of Confidential Data:**

|  |  |
| --- | --- |
| PC/Mac/Laptop: | Ensure an explicit username password is needed to log on. Consider using a power on password to deter theft of remote data. |
| External hard drives / removable devices / USB sticks: | These devices should be encrypted. |
| Tablet/Phone/Ipad: | Storage should be encrypted and a passphrase should also be required to access the information. |
| Emails / email attachments: | Emails can be easily intercepted and read. Any attachments should be encrypted. |
| Cloud/Dropbox etc: | Internet document transfer tools can be vulnerable. The School provides explicit guidance to the use of these internet based programmes at <http://www2.lse.ac.uk/intranet/LSEServices/IMT/guides/softwareGuides/other/using-dropbox-cloud-based-services.aspx> |
| Travelling with encrypted confidential data: | Some countries may demand that you hand over your encryption keys. Check before you travel and contact the Information Security Manager for further information. |

**Storage of Confidential Data:**

*Electronic data:* the storage of data classified as confidential differs from that of critical data. Check the data classification policy, and if you need further help or advice on storage contact the IMT IT Service Desk.

*Physical data:* Hard copy records that require protection for business continuity purposes will have the following characteristics:

* They are originals
* They have legal status
* They relate to outstanding payments to the School
* They are handwritten, or mainly handwritten
* They are in ledgers

To safely store it consider the following methods:

* Make sure you store your data in a secure location that is fire and water proof.
* Consider investing in a fire proof document safe to hold confidential files, such as exam scripts, student loan agreements, contracts etc.
* Store documents in the School’s offsite record repository if they are not in regular use. The Records Manager will be able to advise on this.

**Back Up of Business Critical Data:**

*Electronic Data:*

* Do not store data one place but have multiple copies, on external hard disks or writable DVDs.
* Make sure that you store all copies of your data in a secure location and that material is encrypted and devices passworded.
* Keep paper copies of essential IT records.

*Physical data: (for more information see the website above or contact the Records Manager)*

* Scan critical documents and store electronically.
* Keep back up copies in a secure fire and water proof location, e.g. a safe.
* Have off site back up copies e.g. in the School’s external records depository, or in a securely locked facility in a key team member’s home.

**How Long Should Data be Retained?:**

The School policy on how long data should be retained is outlined here: <http://www2.lse.ac.uk/intranet/LSEServices/legalAndCompliance/recordsManagement/retentionSchedules.aspx>

**Safely Disposing of Business Critical Data:**

At the time of writing the School’s policy on disposal of data has not been finalized. However, you should be aware that just deleting electronic data does not necessarily wipe it off your systems and you may need to overwrite it several times (the US Department of Defence recommendation is 7 times). A free tool such as ‘eraser’ (<http://eraser.heidi.ie/>) can do this.

In terms of physical data, Environmental Services oversee the confidential waste service contract, but it is the porters that can deal with any requests for confidential sacks and organise for their collection and destruction.  The main issues are to ensure that confidential waste sacks are picked up as soon as possible and kept in locked places before being picked up e.g. not in publicly accessible corridors. CDs and DVDs can be cut up but take care that you wrap up any sharp edges or let the cleaners know that they should take care when disposing of rubbish bags containing any shards.

**Good Housekeeping:**All members of staff who create, store, receive and use records must:

* Treat records as a School resource;
* Ensure as far as practicably possible that records are accurate and filed in such a way that they can be easily located;
* Keep records no longer than they are needed;
* Keep confidential records in a secure environment;
* Keep records stored in a safe and cost-effective way;
* Allow people to access information only if they need or have a right to do so;
* Create records that are accurate and that do not defame another individual, expose the LSE to unnecessary risk or to tamper with records in a way that risks them becoming inaccurate;
* Save long term records in an open source or archival format to ensure readability even if systems change

**BUSINESS CRITICAL DATA LOG**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **DATA NAME** | **DATA TYPE**  **e.g. hard copy, electronic etc** | **IS DATA PASSWORDED / ENCRYPTED / SECURE?** | **DATA DESCRIPTION / IMPACT OF LOSS** | **CURRENT LOCATION** | **BACK UP ARRANGEMENTS** | **DATA OWNER** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

ALTERNATIVE ACCOMMODATION

In the event of any situation where access to the <UNIT’s> place of operations is denied, and it is not part of a School wide incident, < *staff and students*> will be informed of alternative accommodation arrangements by <DESCRIBE OR LIST METHODS - *consider also whether staff and students should remain at home or gather elsewhere in the School whilst waiting to be informed*>.

*OR:*

In the event of any situation where access to the <UNIT’s> place of operations is denied, <*staff and students>* should report to alternate locations. Primary and secondary locations are listed below.

**Alternate locations *Workplace: <Name>***

* <describe any special arrangements>

***Workplace: <Name>***

* <describe any special arrangements>

***Workplace:<Name>***

* <describe any special arrangements>

*OR:*

*Detail other alternative accommodation arrangements that apply to your unit, who is responsible for organising them and any other parties you will need to contact within the School to organise them.*

**BUSINESS CRITICAL ACTIVITIES**

*\*Once you have identified and graded your School business critical activities you may wish to look at where you are vulnerable and how you might build resilience into your activities to mitigate the risks should they be compromised. This table is not exhaustive and there may be other information you wish to capture. This template includes a separate table for business critical systems, such as IT systems etc, but you may prefer to amalgamate them into an activities table.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ACTIVITY** | **DESCRIPTION & INTER -DEPENDENCIES** | **CRITICALITY RATING** | **MAXIMUM RECOVERY TOLERANCE** | **DESCRIPTION OF RECOVERY ACTIVITY** | **DESCRIPTION OF ALTERNATIVE ARRANGEMENTS** | **OWNER OF ACTIVITY** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Guide:**

**Activity:** what is the activity? E.g. time tabling, succession planning.

**Description & Interdependencies**: what does the activity do? Where are the inter dependencies: who else is dependent on this activity, who are you dependent on for this activity? Do you rely on other functions for this activity to remain viable?

**Criticality Rating:** how important is this activity, what would be the impact of its loss or failure? Choose a way to grade it, e.g. designate it low, medium, high, essential, use a traffic light system, or rate it on a scale of say 1-10 with 10 representing an activity your unit cannot function without.

**Maximum Recovery Tolerance:** how long can you go without this activity before business activities are severely impaired?

**Description of Recovery Activity:** what does your unit need to do to ensure the recovery of the activity? E.g. contact IT if there is a problem with a system, notify students, rearrange appointments

**Description of Alternative Arrangements:** is there anything you can do to mitigate the effects of the compromised activity, are there other arrangements you can put in place to ensure the unit’s business continues whilst the activity is compromised?

**Owner of Activity:** who is responsible for the activity and for ensuring arrangements are made for its recovery. You may wish to ensure the owner has a deputy in case they are un-contactable or absent during an incident. The deputy should have sufficient knowledge of the activity to know what needs to be done.

**BUSINESS CRITICAL ACTIVITIES CALENDAR**

*Below is a simple table – you may wish to formulate your own calendar and capture other information. (An example of an academic year calendar can also be found on the School’s Business Continuity webpage.) You may also wish to distinguish particularly important processes and activities or where your unit is vulnerable and at what times of the year its activities may be under strain.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **MONTH** | **ACTIVITIES** | **INTERDEPENDENCIES** | **OTHER AFFECTED AREAS** | **OWNER** |
| **JANUARY** |  |  |  |  |
| **FEBRUARY** |  |  |  |  |
| **MARCH** |  |  |  |  |
| **APRIL** |  |  |  |  |
| **MAY** |  |  |  |  |
| **JUNE** |  |  |  |  |
| **JULY** |  |  |  |  |
| **AUGUST** |  |  |  |  |
| **SEPTEMBER** |  |  |  |  |
| **OCTOBER** |  |  |  |  |
| **NOVEMBER** |  |  |  |  |
| **DECEMBER** |  |  |  |  |

**BUSINESS CRITICAL SYSTEMS LOG**

*The most obvious business critical systems are IT based, such as Moodle, Outlook, telephony, and the more specific systems relevant to your unit. However, you may have other systems that enable you to undertake your activities that you need to consider, or there may be systems in other parts of the School on which your unit is dependent. How would you recover them, what would be the impact if you couldn’t access or use them?*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **SYSTEM** | **DESCRIPTION & INTER -DEPENDENCIES** | **CRITICALITY RATING** | **MAXIMUM RECOVERY TOLERANCE** | **DESCRIPTION OF RECOVERY ACTIVITY** | **DESCRIPTION OF ALTERNATIVE ARRANGEMENTS** | **\*OWNER** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**\****you may wish to list not only the person who has responsibility for this system within your unit and who would cover for them in their absence, but also who you should contact in the event of a problem with it, e.g. IT Helpdesk, Payroll contact, ARD contact etc.*

**EXAMPLE OF AN INITIAL ASSESSMENT FORM FOLLOWING AN INCIDENT**

*You may find the following form helpful when you are assessing the impact of an incident. It is not exhaustive and having reviewed it you may wish come up with an alternative layout of your own and questions more relevant to you. Or you may find you do not need it at all. Or you could use it at different stages in your response to an incident to check that you are on course, e.g. immediately after the incident, 48 hours after the incident, 7 days after the incident. The key thing is that it meets the needs of your unit and that it helps you recover the activities that are critical to the business your unit undertakes.*

|  |  |
| --- | --- |
| **Assessment Question** | **Response** |
| Which key staff members of your team are unavailable? For how long? |  |
| Which of your normal work areas are inaccessible but intact? |  |
| Which of your normal work areas have been destroyed, damaged or made unusable? |  |
| Which systems and other resources are unavailable (systems, telecoms, utilities)? |  |
| Which of your area’s critical work-in-progress is lost? |  |
| Which of your area’s critical assets and information have been lost? |  |
| What are your team’s priorities and critical activities? |  |
| What deadlines are imminent? |  |
| Which recovery site/location would best satisfy your team’s immediate requirements (designated recovery site, hotel, home working etc)? |  |
| Which contingency agreements may need to be invoked to support your team’s recovery? |  |
| How many people can work productively at home or mobile for the next few days? |  |
| Are the premises of other higher education institutes or other third parties available for use by your staff and/or students during the next few days? |  |

**CHECKLIST OF STEPS TO TAKE IN THE EVENT OF AN INCIDENT**

*A table form has been provided below, but you may wish to insert a flow chart or formulate an alternative layout that best suits your purposes. The steps included are simply examples and you should populate the table with the necessary steps relevant to your unit. Service Divisions and Academic Departments will clearly have different needs.*

*You may find it useful to split the checklist into timeframes. For example, a checklist of steps to be taken in the first 48 hours following an incident, within 7 days etc, so you have a clear idea not only of what to do, but also where you should be in terms of recovery at particular points.*

*You might also wish to draw up checklists in advance for certain generic scenarios, for example, steps to be taken if you cannot access your premises, in the event of an IT outage etc. These could then be made more widely available to your colleagues so that they are familiar with what your unit will do should there be an incident.*

|  |  |  |  |
| --- | --- | --- | --- |
| **ACTION** | **OWNER** | **DESCRIPTION** | **COMPLETED** |
| Gather as much information about the incident as possible  *e.g what has happened, is it already being dealt with, if so how, have other arrangements been made already, who will be affected or have been affected, is the incident School wide and has the MIIRP been invoked etc?* |  |  |  |
| Notify Head of Dept/Div |  |  |  |
| Contact key people |  |  |  |
| Decide course of action in response to incident |  |  |  |
| Identify impact of incident |  |  |  |
| Identify business activities affected |  |  |  |
| Notify other affected parties  *e.g. students, lecturers, visitors, other units with which you work closely* |  |  |  |
| Identify who within the School should be contacted.  *e.g. IT, Estates, Security, students, lecturers* |  |  |  |
| Identify who should be contacted external to the School  *e.g. contractors, emergency services, local authorities.* |  |  |  |
| Identify business critical activity & commence recovery  *e.g. what activities are most at risk and do they need to be recovered or have alternative arrangements put in place.* |  |  |  |
| Alternative accommodation needed for unit |  |  |  |
| Alternative IT resources needed for unit |  |  |  |
|  |  |  |  |
|  |  |  |  |

**EXAMPLE OF A CHECKLIST FOR AN ACTIVITY OR TASK**

|  |  |  |
| --- | --- | --- |
| Initials / completed | Task to be completed | Owner |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**LESSONS LEARNT/INCIDENT LOG**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Incident Date** | **Incident Description and Impact** | **Description of resolution / recovery** | **Time taken to resolution / recovery** | **Lessons Learnt** | **Recommendations** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |