Ombudsman
Ombwdsmon
PUBLIC SERVICES OMBUDSMAN FOR WALES
OMBWDSMON GWASANAETHAU CYHOEDDUS CYMRU

Business Continuity Plan

Contents

1 Overview

1.1 Aim and objective

Overall aim is to ensure that PSOW returns to effective operation as quickly as possible after a major incident. It is the aim that the office would be back to full operation within 15 working days (3 weeks), following a catastrophic incident which denies the organisation the use of its office and facilities.

This is a live document that will be most effective if it reflects the current position.

1.2 Definition of 'Incident' for the purpose of this policy

For the purpose of this Policy, 'Incident' is defined as any situation that for a sustained period of time prevents the majority of staff from utilising PSOW premises or facilities (general office and/or ITC facilities) thereby having a major impact upon the output of the PSOW as an organisation, such as:

- Unable to enter premises, or premises unsafe or unsuitable e.g. due to flood / fire / other damage etc.
- Unable to access or use PSOW ITC facilities e.g. due to flood / fire / theft / other damage etc.
- Sustained lack of suitable environment e.g. lack of power, heating, running water, toilet facilities.
- Majority of staff unable to attend PSOW premises e.g. Due major transport issues, health reasons such as disease outbreak etc.

Incidents which cause disruption for less than a full working day may be managed without the need for implementation of this policy in full.

2 Business as usual Process

2.1 Business Continuity Policy Review Team

This team will consist of the following;

- Chief Operating Officer & Director of Improvement (COODOI)
- IT Manager (ITM)
- Financial Accountant (FA)
- Head of Corporate Services (HCS)
- Information Governance Manager (IGM)
- Head of Communications & Public Affairs (HOC)
- Other members of staff may be called upon to participate in any testing.

The Review Team is responsible for conducting a test exercise of this policy on a regular basis. The COODOI will decide the scenario(s) to be tested and the test conditions, ranging from basic desktop exercise involving only the Review Team, to fuller testing involving all staff.

In the event of relevant information coming to light between tests, a special interim meeting of the Review Team may be called. This will ensure that any changes are incorporated as promptly as possible. Unless such a process is followed it is likely that in the event of a major incident the documentation available will not be adequate for the purpose. The results of all tests should be presented to Management Team and the

Audit & Risk Assurance Committee.

2.2 Continuity plan location

Whilst this Policy can be located on the PSOW Intranet (The HUB), as with all PSOW policies, in case of lack of IT and/or premises access copies of this Policy are to be held offsite at all times by the ITM and COODOI (e.g. on the PSOW password protected Tablet).

2.3 Information kept up to date

It is important that in the course of normal day to day duties outside of any incident management, the following information is kept up to date.

- **Staff contact details to be kept by Line Managers:** Corporate Services will issue twice a year a full list of all staff contact details, in electronic form, which all line managers must maintain as a pdf document on their PSOW issued portable device (smartphone and / or tablet). Interim contact lists will be issued by Corporate Services upon any significant changes to staff contact details. All staff must inform their line manager and Corporate Services of any change to their contact telephone number as soon as possible. Line Managers are reminded that PSOW issued smartphones and /or tablets must NOT be left in work and must be maintained / charged and ready for use at all times.

- **IT Backup :**
  - **Daily** backups are made and stored in electronic format on-site in the PSOW servers (2 copies – 1 on ground floor server, and 1 on 1st floor server)
  - **Weekly** backups are copied to the portable servers. There are 3 portable servers, two of which are stored offsite (with ITM and ITO), and one onsite in the first-floor server room. The off-site servers are rotated in turn every other week with the on-site server every Friday. This means that there is always one backup server off-site with a maximum Recovery Point Objective (RPO) of 1 week.

- **External contact details:** Corporate Services will maintain an up-to-date database of existing suppliers and their contact details. This is web-based and the HCS and COODOI will have access to this database.

- **Online banking, BACS and commercial banking**: COODOI, FA and HCS must have means of accessing PSOW's bank accounts online (card and card reader) off-site when they are not in the office.

- **Debit cards / Credit cards:** All PSOW issued debit and credit cards are to be kept by the named cardholder and not stored onsite when the cardholder is not present.

3 Recovery Management

3.1 Initial Assessment

If any member of staff is made aware of a potential incident, they must contact the COODOI or ITM immediately (directly or via their Line Manager).

As soon as the COODOI and/or ITM are made aware of an incident they are required to undertake an immediate and initial assessment of the incident and its obvious and immediate implications to the PSOW, and the immediate actions required. This may require a site visit if the incident is out of hours. Dependent upon the seriousness of the incident, it may be appropriate to inform the Ombudsman immediately. The 'Initial Assessment' form (Appendix A) can be used as an aid in this initial assessment.

3.2 Initial Communication

Following this initial assessment, the COODOI / ITM are to decide:

- What exactly to communicate to **Line Managers**

  e.g. 'the office will be closed for an unknown period due to….. All line managers to contact everyone in their team to inform. Please contact me back to confirm when done'.

  The ITM is to collate names of staff that have not been contacted and consider what further contact attempts can be made.

- What should be communicated **to staff** via the Line Managers

  e.g. 'the office will be closed for an unknown period due to…. The Line Manager will contact you later in the day with an update.'

- When to begin the information cascade

  e.g. If the incident occurs out of office hours, it may not be necessary to contact Line Managers and or instruct them to contact their staff immediately.

Information will need to be cascaded initially to the Line Managers (and Ombudsman if not already informed). Line Managers are then responsible for cascading this information to all staff within their teams (including any Agency Staff and Investigation Associates).

In the event that the COODOI or ITM are unable to contact a Line Manager, it is not appropriate to leave a request to cascade the information in a message. The COODOI and ITM are responsible for ensuring the relevant members of staff are contacted in this instance.

Messages may be left by Line Managers for their staff, but it must include a request to acknowledge back to the line manager. Line Managers must contact the COODOI / ITM after contacting their team to confirm names of staff who may not have had the communication.

If possible, Line Managers are to also inform the ITM of any expected visitors to the office (including IPAs). The ITM will then try to contact the visitors prior to the meeting to cancel / postpone.

3.3 The Recovery Team

- **The Recovery Team Managers:** In addition to the Ombudsman taking a strategic overview role, the COODOI will be the lead Recovery Manager with the ITM acting as his deputy.

- **The Recovery Team** will also consist of the Chief Legal Advisor & Director of Investigations, Investigation Managers, Information Governance Manager, Head of Communications & Public Affairs, Financial Accountant, Head of Corporate Services, Head of Casework Support, IT Officer, Data Reporting Officer, Corporate Services staff and any other members of staff suitable for the incident, as deemed necessary by the Recovery Team Managers.

- **Control Centre:** A control centre will need to be established to initiate and manage a recovery plan. The control centre will be based at a location deemed suitable and available dependent upon the circumstances (this may be PSOW offices if any part is accessible / safe / useable). The Recovery Managers are responsible for agreeing upon this location.

4 The Recovery Plan

Appendices B and D are to be used as a checklist for any recovery plan.

4.1 Secondary Assessment

Following the setup of the control centre, the Recovery Team are to review the initial assessment of the incident regarding the expected effects, the expectations of what is required to be done to effect full recovery and the estimated timescales.

Protection of information and Assets: If there is a risk of any unauthorised access to premises due to the incident the following should be performed assuming access has been deemed safe (following authorisation from emergency services if relevant);

- ensure the premises is secure – enlist a security company if necessary
- safeguard all data on computers
- remove/secure any equipment remaining on site
- remove/secure any documentation remaining on site

4.2 External Communications

Consideration of what to and how to communicate externally is required to be undertaken by the recovery team. It is essential that a uniform message is agreed by the recovery team and that this must be following full consultation with the Head of Communications & Public Affairs (HOC) or a member of the communications team in the absence of the HOC.

- **The Public and Relevant Bodies:**

  - **Telecoms** - It is essential that the Ombudsman telecom suppliers are contacted to enable an interim message to be communicated to all callers who try to access the Ombudsman's telephone line numbers. (01656641150, 01656641160, 08456010897, 03001231299, and individual staff direct line numbers)

  - **Website** - A communication needs to be posted to the Ombudsman's website(s) relating to the possible interruption to services provided by the Ombudsman and any alternative contact routes if known.

  - **Post** - Collection and delivery, including redirection needs will need to be arranged to minimise any delay, possible missing items or items returned to sender unnecessarily. The Post Office Collection Reference for 1 Ffordd yr Hen Gae is FIR816276.

  - **Relevant Bodies** – Corporate Services will maintain offsite a list of relevant bodies and appropriate contact details. The recovery team will draw up an action plan for contacting these relevant bodies and in what order, dependent upon the circumstances.

- **The Media / Sister Organisations** The Head of Communications & Public Affairs (HOC) is responsible for setting up and overseeing the implementation of an action plan for relevant communication to the Media, and Sister Organisations and other relevant persons / organisations as deemed relevant by the Communications Team based upon the circumstances.

PSOW Main suppliers / service providers. The Recovery Team can commence contacting the Major Service suppliers to PSOW, to inform them of the incident, temporary contact details and the possibility of stopping services temporarily if applicable and possible. The first contacts that should be made are: IT (CAS, internet/broadband suppliers, IT Support providers), Communication links (telephone), Postal services, Bank/finance, Landlord.

4.3 Premises

As PSOW is mainly a one site office, any disruption to access or suitability of the premises for a sustained period of time would effectively result in the inability of this office to carry out its core function in any significant manner.

The Recovery Plan regarding premises would need to take into account the expected duration of the lack of use of the main PSOW Premises, and also the severity of the lack of access.

Severity: Can any part of the premises be used safely? If so, can this be utilised to carry out key functions or possibly more on a temporary basis.

Duration: Is the duration of the lack of premises short term, medium term, or long term / indefinite?

Based upon the answers to the above, a decision would then need to be made as to whether to carry out one or more of the following;

- Close office temporarily with no core function duties being carried out.
- Skeleton staff only in available PSOW office space.
- Enable staff to work from home via remote access (assuming IT services intact)
- Procure temporary office space (with appropriate IT and Telecoms)
- Procure permanent replacement premises and facilities.

If temporary office space is considered appropriate, managed office space will be needed to accommodate the current staff headcount of PSOW. Temporary office space providers can be sourced via the internet.

As well as the managed office space there will be requirement for (if not already included in the office space provision):

- Workspaces/desks/chairs adequate for current PSOW staffing requirements
- Communication links
- Computer points to match staffing requirements
- Office management facilities; photocopiers adequate to meet current

requirements; postal franking machine; telephones adequate for current PSOW staffing requirements

- Car parking facilities for staff where possible
- IT equipment adequate for temporary purpose.
- Initial office stationery equipment and supplies.

4.4 Utilities

For outages affecting power / lighting / heating and water, the COODOI, HCS and ITM must assess the likely duration of the outage and then make an informed decision as to what actions are to be taken in the immediate short term. It is envisaged that alternative arrangements can be made for unplanned water outages of 1 day or less, and brief outages for power / lighting / heating may be managed locally dependent upon the circumstances and environmental conditions that apply at the time.

For outages exceeding 1 day an action plan must be drawn up detailing what arrangements can be made to minimise / eliminate the effects on PSOW service.

4.5 ICT facilities

All aspects of the computer systems must be coordinated through the current IT support service provider and ITM and ITO/DRO in support.

To minimise the loss of IT due to hardware failure, the servers are copied to mirror servers on site regularly throughout the day. If any servers fail (hardware failure), server access is re-routed to the mirror servers with negligible impact to the operation of IT systems.

In the event of software corruption which has been copied to the mirror servers, data can be recovered from either the daily backups to the backup servers, or the off-site portable server backups. A worst-case scenario would be 5 workings days loss of data in event of the on-site daily backup being unrecoverable from the premises.

In the event of complete hardware failure or loss then the following are in place:

- Detailed specifications for the hardware and a Register of the software are held by PSOW ITM Offsite. Specification for replacement servers which can recover the information from the backup servers is part of the hardware specification.

- An Escrow agreement is in place for all content and content management functions of the Ombudsman’s websites managed by Fusion Ltd.

- An Escrow agreement is in place for the WorkPro content management software.

All other software and hardware are commercially available.

4.6 Financial

- **HR and Pay information**
  The most recent off-site backup computer files will provide the key data. It will be necessary to obtain that key data as soon as possible after the incident has occurred.

Recent salary payment details can be accessed remotely through on-line commercial banking. This will enable salary payments to be made (based on a previous month's data) if pay is due.

- **Banking**

  Bank emergency arrangements:

  - These will generally rely on use of PSOW debit and credit cards and on-line banking.
  - New cash requisition paperwork, including contact details for obtaining cash requisition from Welsh Government will be held by the Financial Accountant off-site and secure.

- **Accounting information**

  Whilst paper documentation may no longer be available, all up to date, day-to-day operational accounting information will be available from the most recent backup. The possible delay in accessing this back up data is not deemed sufficient to impact on the Ombudsman's ability to operate.

  Essential Financial Information as defined by Financial Accountant is recoverable from the National Assembly website (e.g. annual financial accounts and estimates for current year). This information is available on the website of the Finance Committee of the National Assembly for Wales and on the Paid documents details again held on the same website.

Document Owner	COODOI
Policy & EIA approved by management team	Policy revision & revised EIA approved by Management Team12 November 2019
Due date of next Review	Upon revised DR systems implementation.
For publication to :	Intranet (YES) PSOW website (No – not a public document due to sensitive information on what is stored offsite)

Appendix A

Business Continuity Initial Assessment Form

Description of incident (including reasons if known)	Start Time & Date of issue	Estimated end time & date of issue (if known)

Services Affected	None / Partial / full	Comment on anticipated duration of service failure
Road /Rail / Public Transport		
Staff resources		
Access to Premises		
Car parking		
Premises		
Power		
Heating / air conditioning		
Lighting		
Door security		
Water		
Toilets		
Internal IT (hardware / Software / network / wifi)		
External IT (i.e. websites)		
Telephones		

Comment on overall impact of above
COODOI / HCS / ITM Agreed actions (e.g. full implementation of Business continuity plan)

Business continuity Action Checklist APPENDIX B

Action	Action Owner	Deadline	Completed (Y/N)
Initial Assessment (Appendix A)	COODOI / HCS / ITM	Day 1	
Control centre established	COODOI / HCS / ITM	Day 1	
Initial Communication to Management Team & Line Managers	COODOI / HCS / ITM	Day 1	
Communication to Recovery Team	COODOI / ITM	Day 1	
Commence IT DRP (see appendix E)	ITM	Day 1	
Confirmation from line managers of Communication to Staff	Line Managers	Day 1	
Secondary assessment • Site visit – damage assessment • Emergency services review • Site security requirement • IT functionality • Salvage assessment (IT & Non IT)	COODOI / HCS / ITM	Day 1/2	
External Communications (services) • Email server message • Landlord • Telecomms action list o Divert all ext to main line o Emergency message on main line • Website o Emergency message • Post • Bank • Relevant Bodies • PSOW main service providers	ITM/HCS/ HOC	Day 1/2	
External Communications (RB/Media) • Media • Sister organisations	HOC	Day 1/2	
Action plan devised for recovery and repair or replacement for affected services / premises.		Day 3/4	
Action plan devised for temporary service until fully recovered (e.g. temporary premises)		Day 3/4	
Action plan devised for staff return to work			

Implement above action plans and communicate to staff at relevant points (e.g. initially once action plan agreed, then after securing start date of relevant premises and required service infrastructure)			

Business Continuity Testing Form Appendix C

Test scenario	
Test condition (e.g. ranging from desk top exercise by COODOI/HCS/ITM only to full realism scenario involving all staff)	
Simulation of … e.g. flood	
Service	Test condition level of availability (i.e. full / partial or none), and until when?
Site Access / Transport	
Staff Availability	
Premises Access	
IT networked services (WorkPro / intranet / emails / drives, Tablets, Smartphones etc.)	
Telecomms services • Office landlines • PSOW mobiles • Broadband	
Utilities (Electricity/ Water / Heating)	

Other test conditions	
Access to data / information	**Comments**
Availability / Access to Business Continuity Plan	
Key data access • Access to online banking, including staff pay and bank details • Access to debit and credit cards • Access to web-based supplier database	
ICT back up data access: • Access to most recent offsite portable hard drive back ups • Access to servers • Access to CAS and IT Support providers	
Control centre agreed & established	
Access to contact details of Recovery team	
Information cascade step 1: Access to contact details of management team	
Information cascade step 2: Line managers access to contact details of their team	

Information cascade step 3: Recovery team access to all staff contact information.	
Comments on completion of Business continuity action checklist (appendix B):	
Signed……………………………………………Date………… **Signed……………………………………………Date…………** **Signed……………………………………………Date…………**	

Business Continuity key information location Appendix D

Key information	Soft copy		Hard copy		Update frequency
	Onsite	Offsite	On site	Off site	
Continuity Plan policy	PSOW intranet	Yes – on PSOW issued tablets in PDF reader folder	No	No	As per policy updates
Management Team and Business continuity recovery team members' contact details (excluding next of kin / emergency contact details)	Sage HR via corporate services PCs only	Members of Management Team and Recovery Team will hold contact details of the other team members on their PSOW issued Smartphones	No	No	Upon any change
Possible emergency control centre locations	Recovery Managers to discuss and agree upon notification of event (i.e. based at the home of a member of staff or other suitable and immediately available location)				
Possible formal medium-term control centre locations and / or alternative premises for PSOW staff	Relevant information to be sourced via online search				
Team contact lists (excluding next of kin / emergency contact details)	Sage HR via corporate services PC's only	Each line manager will maintain contact details for each of their team on their PSOW issued Smartphones	No	No	Upon any change
All Staff contact list (including next of kin details)	Sage HR	With COODOI and ITM issued 6 monthly and stored on tablets	No	No	6 monthly or Upon any change
Corporate Services contacts - Priority	Web-based supplier database & Business Continuity Plan	Web-based supplier database & Business Continuity Plan	No	No	As per any changes
Corporate Service contacts – non priority	Web-based supplier database & Business	Web-based supplier database & Business Continuity Plan	No	No	NA

Key information	Soft copy		Hard Copy		Update frequency
	Onsite	Offsite	On site	Off site	
Bank Account & Debit card details	No	No	Actual Card	HCS	Upon any change
Financial Accountant. accounting data	PSOW Intranet	National Assembly Website	No	No	As per any changes
List of IT assets (including IT specifications and software licence register)	PSOW Intranet	Offsite with onsite IT support provider	No	No	Annually
Cash requisition forms	PSOW Intranet	Electronic copy stored locally on FA tablet	No	No	As per any changes
PSOW Act and published PSOW policies	PSOW Intranet	PSOW Website	No	No	As per any changes
Most recent net pay wages amounts and staff banking details	Lloyds Bank Commercial Banking	Lloyds Bank Commercial Banking	No	No	Ongoing
Weekly back up hard drive	Server soft back ups	Portable server Rotated between ITM and ITO	No	No	Weekly
Daily back ups	Server soft back ups	No	No	No	Daily
Relevant bodies contact list	Workpro Report	PDF file to be stored on Comms team tablets.	No	No	WorkPro report 6 monthly

Corporate Services Contacts – Priority list					
Category	**Organisation**	**Telephone**	**Email**	**Address**	**Contact Name**
Telecoms’	Datasharp	01872 266660			
Website	Spindogs	02920480720			
IT support	Rock IT	03442722292			
WorkPro	CAS Ltd	01312972141			
Bank	Lloyds Bank – Business banking (Gloucester)				
Intruder alarms	Chubb				
Postal	Royal Mail				
Landlord agents / Fire Alarms	Second Horizon				
Other tenant	Macmillan Cancer Research				
Other tenant	Davies Turner Ltd				
Other tenant	NHS-Delivery Unit				

Media /Sister organisations contact list

Category	Organisation	Telephone	Email	Address	Contact Name

Appendix E: IT DRP (commences day 1 of Business Continuity – see appendix A checklist)

1. **Immediate actions**: Notify the following as soon as disaster event has been identified and arrange further secondary callback (after all section 1 actions have been taken) to discuss exact requirements.
   - Notify IT support providers and arrange call back after section actions completed
   - Notify Website providers
   - Notify CMS providers
   - Notify Telecoms providers and schedule any necessary service connections. Arrange emergency message to be played (bilingual) in event of anticipated loss of telecoms / or resource availability
   - Notify Power providers and schedule any necessary service connections.

2. **WEBSITE:** Disable online complaint form and post website message to both English and Welsh websites:
   'Due to circumstances outside of our control, the services of the Public Services Ombudsman for Wales are currently not available. Please note that this affects our ability to respond to emails and telephone calls. We apologise for any inconvenience this may cause. We hope to be able to resume services as soon as possible'.

   [Welsh translation of above required]

   Publish the above message on the main home screen emergency message area, but also the contact us pages

3. **Secondary contact with IT support providers:**

   Discuss / consider the selection of appropriate recovery plan and agree action plan:
   - Is IT recovery possible using onsite back up / mirror server data?
   - Is IT recovery possible using on site servers?
   - Is there a requirement to recover from offsite back up portable servers?
   - If necessary, confirm hardware requirements for initial and full recovery, and arrange procurement

   Provide an equipment delivery site address (when applicable), a contact, and an alternate contact for coordinating service and telephone numbers at which contacts can be reached 24 hours a day.

   RTO time countdown begins at the time IT support providers are notified of recovery plan selection.

4. **Secondary contact with CMS providers**

   Discuss need to reinstall Workpro application and inform of plan from section 3 above.

5. **Meet with PSOW Recovery Managers** to discuss operational options and agree IT requirements (based on IT action plan) for Operational action plan.

   - Are we able to recover to full capacity quickly?
   - Is there a requirement for a staged approach to recovery e.g.:
     1. Key support IT access (IT/Corporate services/Communications)
     2. Reduced CAT telephone cover
     3. Reduced CAT CO cover
     4. Reduced Inv team cover / Reduced Improvement Team cover / Reduced Casework support cover
     5. Full Capacity (all teams or team by team staged)
   - Agree approach to software applications recovery (i.e. stage and priority order):
     1. Emails (MS Office)
     2. Shared drive (for temporary documents)
     3. Accounts / Payroll
     4. HR
     5. Workpro
     6. Telecoms
     7. HUB
     8. Kelio

6. Manage and monitor IT aspects of action plan. Constantly liaising with Recovery Managers and Recovery Team

7. Upon completion of action plan, review and report to Management Team.