SCOTTISH
PUBLIC
SERVICES
OMBUDSMAN
People Centred | Improvement Focused

Business Continuity

Only the Ombudsman and Communications and Engagement Manager may comment to the media when the Incident Response Plan is activated.

Version	***Description***	***Date***	***Author***
1.0	Published on SPSO website	2010 Feb	Corporate Services Manager
1.1	Audited	2012 Jul	Internal Auditor
2.0	Published on SPSO website	2012 Aug	Senior Personal Assistant
2.1	Reviewed	2013 Jun	Senior Personal Assistant
3.0	Reviewed and published on SPSO website.	2015 May	Senior Personal Assistant
3.1	Audited	2015 Aug	Internal Auditor
4.0	Reviewed and published on SPSO website	2016 Nov	Corporate Services Manager
4.1	Updated and published on SPSO website	2017 May	Corporate Services Manager
5.0	Reviewed, audited and published on SPSO website	2019 Aug	Corporate Services Manager
6.0	Reviewed, audited and published on SPSO website	2022 Apr	Corporate Services Manager
7.0	Reviewed, audited and published on SPSO website	2023 Nov	Corporate Services Manager
8.0	Reviewed, updated and published	2024 Sep	Corporate Services Manager

Contents: Business Continuity

Business Continuity Policy

Contents

Back to the main Contents page

The Scope of the policy

1. This policy outlines the SPSO approach to ensuring our business continuity to meet our Strategic Aims in the event of a major disruption to service affecting the normal business activities undertaken by the SPSO in the delivery of our statutory functions.

2. It is acknowledged that there is very little that the SPSO does, with the exception of Scottish Welfare Fund Crisis Grant reviews, which is so critical that public life would be severely disrupted if that activity could not be undertaken for a prolonged period.

3. The policy references the Incident Response Plan (IRP), which outlines what procedures will be followed to ensure the health and safety of staff and to protect the public; and secure prompt and efficient recovery of critical business operations to minimise the disruption to service users and restore business as usual activities as soon as possible.

4. The policy and the plan have been approved by the SPSO Leadership Team (LT) and is owned by the Ombudsman as Accountable Officer.

5. The Incident Response Team (IRT) have their own electronic or paper copy of the full handbook available to them outwith the business premises. A further copy is deposited electronically with the Scottish Parliamentary Corporate Body (SPCB). A redacted version is published on the SPSO website.

Assumptions

6. The following assumptions have been applied to this plan to measure how critical the major disruption is to the business:

Business area and recovery time Critical = Red 🟥 Severe = Orange 🟧	1 hr	4 hr	24 hr	48 hr	1 wk	2 wk	4 wk
Emergency comms – call tree	🟥	🟥	🟥	🟥	🟥	🟥	🟥
ICT Systems – VOIP telephony	🟥	🟥	🟥	🟥	🟥	🟥	🟥
ICT Systems –SCOTS network		🟧	🟥	🟥	🟥	🟥	🟥
ICT Systems – Casework Management System		🟧	🟥	🟥	🟥	🟥	🟥
Governance		🟧	🟥	🟥	🟥	🟥	🟥
External comms – website, social media		🟧	🟥	🟥	🟥	🟥	🟥
Casework - Scottish Welfare Fund		🟧	🟥	🟥	🟥	🟥	🟥
Casework - First Contact				🟧	🟥	🟥	🟥
Casework - Independent National Whistle-blowing Officer				🟧	🟥	🟥	🟥
Casework - Public Service Complaints						🟧	🟥
Corporate Services – HR (Moorepay)				🟧	🟥	🟥	🟥

Business area and recovery time Critical = Red Severe = Orange	1 hr	4 hr	24 hr	48 hr	1 wk	2 wk	4 wk
Corporate Services – Finance (Bank)					🟧	🟥	🟥
Mail and Couriering activities							🟧

7. Impact on the business activity could be:

7.1. loss of internal communication channels for more than one hour could result in mis-direction, confusion, or even panic amongst staff members;

7.2. loss of ICT systems would severely impact all areas of the organisation and becomes more critical the longer it continues from 24 hours downtime. Loss of the SCOTS network and services would critically threaten the SPSO’s ability to carry out its corporate services functions function and meet financial obligations.

7.3. one working day without CMS access may have serious implications for Scottish Welfare Fund (SWF) review process that may result in unnecessary discomfort for vulnerable citizens;

7.4. one working week without CMS access may impede the reporting of life-endangering actions through Independent National Whistleblowing Officer (INWO);

7.5. one month without the CMS and SCOTS Connect service would critically threaten the SPSO's ability to carry out its statutory functions, and the whole organisation will be in a severe situation with potential long-term effects; and

7.6. a catastrophic incident to an external body under jurisdiction or the postal service may impact on complaint investigations, and may have a detrimental effect on vulnerable citizens accessing our service.

Risk assessment

8. The assessed impact to the organisation of a critical incident remains low due to the following mitigating arrangements which ensure the SPSO's ability to respond flexibly and continue to carry out its statutory functions. Any change to these arrangements may be reflected in a change to this assessment.

Office space

9. The SPSO response to the Government imposed lockdown to address the spread of COVID-19 in March 2020 demonstrated the organisation's resilience, and that the

loss of property or access to office space now presents a negligible risk to SPSO's ability to meet its statutory functions.

10. All staff members are equipped with Scottish Government secure laptops, providing the facility to work on the SWAN secure network from an alternative location. Very few activities require to be performed within an office-based environment.

11. Should there be an incident where the office is completely inaccessible, the minimum requirements to continue business as usual would be an alternate address for the receiving and dispatching of mail and couriered materials. In addition, a multi-function machine would be required to enable scanning of the received documents.

Cyber Security

12. The Scottish Government's Cyber Resilience: Public Sector Action Plan encourages all Public Sector organisations to put in place appropriate cyber incident response plans as part of wider response arrangements, and ensure these are aligned with Scottish Public Sector Cyber Incident Central Notification and Co-ordination policy. The SPSO plan can be found here: 220510 Officeholder Cyber Incident Response Plan (A37915672)

13. The purpose of this plan is to provide operational structure, processes and procedures to Officeholder staff based in Bridgeside House, so that they can effectively respond to incidents that may impact the function and security of business operations.

Network:

13.1.1. The loss of our secure network hosted by the Scottish Government would cause the most wide-spread impact on the organisation's ability to meet its statutory functions. This would be due to the loss of access to our general email functionality and the non-casework electronic document management system.

13.1.2. Should there be an incident where we lost access to the secure network hosted by the Scottish Government affecting the delivery of SCOTS Connect services, the iTECS Business Continuity Plan (BCP) may be invoked. This BCP provides for the restoration of the business functions and services provided by iTECS, with appropriate recovery actions depending on the nature and impact of the incident. iTECS involvement would be limited to best endeavours in the restoration of SCOTS Connect services for that customer. iTECS can make no specific commitment to restore customers' SCOTS and other IT Services, nor to the level of prioritisation that would be applied to organisations in the event of an incident. The level of prioritisation would be assessed in line with the incident and business requirements. Support for iTECS customers' own BCPs is outwith the scope of the iTECS plan.

iTECS
Resilience.docx

Cloud-based applications:

13.2. Other corporate management information systems may be accessed on any network solution through website portals. These include: the Human Resources application; the banking application; the telephony system; and SPSO external website.

Case Management System:

13.3. Our CMS (Workpro) is located on a secure cloud-based hosting platform, behind a firewall, that is usually only accessible by site to site VPN from our SCOTS secure network. It is hosted in the Contractor's private cloud and is not exposed directly to the internet. Only authenticated traffic from the secure network can traverse the VPN and access our Workpro sites. Additionally, our public facing web services are locked down to only accept connections from our production and dev web servers.

13.4. The CMS has twenty four seven proactive Cyber Security monitoring to protect against and respond to external and insider threats as well as a second standby data centre to supplement the resilience of the primary data centre.

Workpro%20inform
ation%20security.dc

13.5. Following a critical incident that affected access via the secure network, individual VPN accounts could be in place within four working hours for the minimum required number of users to access Workpro. Medium-term arrangements could include site-to-site or site-to-cloud secure connections as agreed.

13.5.1. If the cloud or other infrastructure that supported the CMS failed, the contractor has given assurance that service could be resumed within six hours through their own BCP. We are on the standard package for restoration.

13.5.2. The Recovery Point Objective would be the hourly for the current day, to the start of each day for the preceding thirty days, or to the start of each month for the preceding two months.

13.5.3. The last three months of overnight backups are stored in an encrypted format, are immutable, disconnected from the platform and copied to a second data centre for resilience. The recovery of SPSO backups is tested by the CMS supplier annually.

VOIP:

13.6. Our voice-over-internet-protocol telephony (VOIP) is a separate system from our IT networks, and allows us to divert our telephone numbers quickly and easily to any alternative handset as required as long as there is an internet connection. Should our VOIP system fail, then we will revert to our contractor's business continuity plans.

240930%20IPEX%20
-%20Business%20Cc

Deliveries:

13.7. Should there be a catastrophic incident effecting the postal service limiting the accessibility of our organisation, an alternative provider would be sought for outgoing mail. Daily service updates are provided on the Royal Mail website.

Resource decisions

14. The basis of any resource decisions would include consideration of the following:

Priority:

15. In the event of a critical incident where access to resources is limited, IRT members must have first priority to enable a smooth response to the incident, then the SWF team will be prioritised.

Minimum resources:

16. In addition to the IRT members, the minimum number of staff that would be required to ensure the SPSO continued statutory operations while recovering from a critical incident are assessed as follows:

16.1. one Leadership Team member;

16.2. two Scottish Welfare Fund Case Reviewers;

16.3. two Assessment and Guidance members;

16.4. six Public Service Complaints Reviewers;

16.5. one Independent National Whistle-blowing Officer Complaints Reviewers;

16.6. one general Corporate Service member;

16.7. one Improvement, Standards and Engagement Comms member;

16.8. one other Improvement, Standards and Engagement member; and

16.9. with management provided by three line managers who may be included in the above numbers, one of which is a casework manager.

17. It is probable that many staff members may often have their laptops safely stored off-site with them when out of the office, particularly if working from home is a usual practice for them. Additionally, with any forewarning of an impending incident, staff will be able to take their devices home during the preparatory and initial response stage. This will enable flexible working arrangements to be in place while there continues to be access to a network. If a laptop is not with the staff member at the time of an incident, arrangements for transporting laptops to staff, or acquiring replacement devices, can be put into place quickly.

Roles and responsibilities

18. When responding to a critical incident the SPSO has adopted the same command and control structure as the UK emergency services to embrace the full staff structure:

Level / Role	Members	Areas of Responsibility
Gold **Strategic:** **Ombudsman+** **Hand off** – overall view of the incident, provide leadership, commitment and resources as part of governance	• Ombudsman • Head of Corporate and Shared Services (+ IRT Director) • Head of Improvement, Standards and Engagement	• overall aims, objectives and strategy for the incident • media strategy and handling the reputation risks • decisions affecting the whole organisation • financial and resourcing considerations • medium-term planning
Silver **Tactical** **Incident Response Team (IRT)** **Hands in** – respond to incident, how to coordinate the response. Directing the operations level and working towards the strategic objectives	• IRT Director - Head of Corporate and Shared Services • IRT Manager - Corporate Services Manager • Deputy IRT Manager - ICT Systems Analyst and Building Coordinator • IRT Support - Communications and Engagement Manager; HR Manager; Head of Investigations	• develop and deliver an effective business continuity plan, including facilitating training and testing essential points of the plan • responsible for activation and management of the Plan • ICT - establishing a replacement telecommunications network and IT service, cyber security • media and external communications - communicating with local and national media and for establishing a response centre

Level / Role	Members	Areas of Responsibility
		• Human resources and internal communications - staff welfare • building and WFH - Health, safety and security considerations • management of casework related actions to retain minimum activity to meet statutory requirements • emergency financial payments
Bronze **Operational** **All staff** **Hands on** – doing the response on the ground	• Corporate Services Team members • Comms Team members • Managers and Team Assistants • other staff members as required	• understand relevant plans and associated roles and responsibilities • recognise an incident and alert IRT/manager - escalate as appropriate • respond to instructions and perform tasks as instructed by IRT, LT or line manager

Incident response team (IRT)

19. The IRT is responsible for providing overall direction of the incident recovery operations. The role of the IRT is to:

19.1. consider impacts of the incident

19.1.1. evaluate of the extent of the problem and the potential consequences
19.1.2. initiate business continuity procedures
19.1.3. activation and deactivation of the plan

19.2. liaise with emergency services

19.3. take decisions on essential products or services and current work priorities

19.3.1. manage available resources
19.3.2. monitor control of emergency expenditure
19.3.3. ensure maintenance of security
19.3.4. maintain external public relations

19.4. monitor and report recovery progress.

20. The IRT is made up of:

Role	Deputy	Responsibilities
IRT director • Head of Corporate and Shared Services (HoCSS)	• CSM	• Receive and assess impact assessments • Consider if the BCP should be activated • Chair IMT meetings • Take decisions on allocation of available resources

Role	Deputy	Responsibilities
IRT manager - Corporate Services Manager (CSM)	- HoCSS	- Ensure communication with affected staff is maintained - Assess and communicate current priority activates to staff - Ensure actions are carried out - Ensure contingency arrangements are in place
Deputy IRT managers - ICT Systems Analyst (ISA) - Building Coordinator (BC)	- TA – ICT / Finance	- Logs actions on behalf of the Plan Owner - Assist with coordination of the incident on behalf of the Plan Owner - Assists with administrative support
IRT support - Communications and Engagement Manager (Comms) - Human Resources Manager (HRM) - Head of Investigations (HoI)	- Omb - HoCSS - HoI	- Responsible for specific role-related activities

IRT specific responsibilities during a critical incident

IRT Director

Head of Corporate and Shared Services
Deputy: Corporate Services Manager

1. Take overall responsibility for management, control and activation of the Plan.
2. Receive and assess impact assessments.
3. Chair IMT meetings.
4. Take decisions on allocation of available resources.

IRT Manager

Corporate Services Manager
Deputy: Head of Corporate and Shared Services

5. Ensure communication with affected staff is maintained.
6. Assess and communicate current priority activates to staff.
7. Ensure emergency financial payments can be made, including setting up and maintaining budgetary control procedures for emergency costs and maintaining records of expenditure for subsequent insurance claims.
8. Actions are:

   8.1. initiating the call chain procedure;
   8.2. identifying support staff to assist with incident response; and
   8.3. contacting contractors.

Deputy IRT Manager

ICT Systems Analyst or Building Coordinator
(depending on incident and other support required)

9. Logs actions on behalf of the Plan Owner.
10. Assist with coordination of the incident on behalf of the Plan Owner.
11. Assists with administrative support.

IRT Support

ICT Systems Analyst
Deputy: Team Assistant – ICT and Finance

12. Establish a replacement telecommunications network and IT service by liaising with IT services providers to:

    12.1. provide standby IT facilities to the agreed level of service to business-critical users;
    12.2. reinstate normal IT services with the predetermined timescale; and
    12.3. configure new hardware, software and communications facilities and ensure that the integrity of data is safeguarded.

13. Actions are:

    13.1. ensuring messages are applied to telephone lines, website, building, etc.
    13.2. make arrangements for the reinstatement of IT and telephony services - ensuring ICT Service providers do the following:

        13.2.1. establish procedures and schedules for the operation of standby facilities;
        13.2.2. install operating systems, application software and data on standby and replacement IT facilities;
        13.2.3. retrieve documentation and media from backup storage;
        13.2.4. implement interim processing and backup procedures;
        13.2.5. enforce logical security at the standby site;
        13.2.6. initialise and test standby hardware, operating systems and communications;
        13.2.7. contact suppliers and order and configure replacement facilities; damage evaluation, identification of salvage, removal of re-usable equipment;
        13.2.8. provide information and support for interim IT facilities; and
        13.2.9. reconfigure the communications network as required and monitor performance.

Building Coordinator
Deputy: Corporate Services Officer

14. Responsibility for health, safety and security, building repairs and general administration including the reinstatement of normal building services within the predetermined timescale. If required, finding alternative accommodation facilities for essential in-office functions.

15. Actions are:

15.1. implementing health and safety protocols;
15.2. contacting the appropriate authorities to ensure that the affected site is made secure to prevent unauthorised access by staff or the public;
15.3. setting up and maintaining all administrative support services such as receipt and distribution of mail and couriered items, telephone, office equipment, etc.; and
15.4. organising for documentation and equipment to be transported securely.

Communications and Engagement Manager
Deputy: Ombudsman

16. Media and External Communications - responsible for the implementation of the Critical Incident Communications arrangements, including communicating with local and national media, and for establishing a response centre.

17. Actions are:

17.1. ensuring a response centre telephone facilities are set up;
17.2. drafting press statement and communicating with media;
17.3. updating SPSO website and social media with statement to service users/the public;
17.4. monitoring media and social media;
17.5. logging all media calls; and
17.6. ensuring staff know that media enquiries are directed to Communications and Engagement Manager.

HR Manager
Deputy: Head of Corporate and Shared Services

18. Human Resources and Internal Communications - responsible for staff welfare.

19. Actions are:

19.1. dealing with any staff problems caused by the disaster and handling front-line communications with staff and their relatives.

Head of Investigations
Deputy: Head of Investigations

20. Management of casework related actions and distribution of resources to retain minimum activity to meet statutory requirements.

21. Actions are:

21.1. ensuring the least amount of disruption to casework functions caused by the disaster;
21.2. coordinating staff and available resources to maintain maximum effectiveness with available resources; and
21.3. arranging for the secure transportation of hardcopy casefiles to the available case reviewers as appropriate.

Testing and maintaining the plan

22. The IRT will meet annually to review their roles in the plan, talk through the possible scenarios, test elements of the Plan, and complete the Business Continuity Checklist.

23. The checklist will be used to ensure important elements of the Incident Response Plan are current and correct. This includes:

23.1. testing the Call Chain Procedure annually; and
23.2. reviewing emergency contact details each year and updating where necessary.

24. Test results will be documented and reported to the Leadership Team annually through the Corporate Services Assurance paper.

Back to the main Contents page

Disruption to work – further policy information

Contents

Back to the main Contents page

1. This policy is for all SPSO staff and contractors.

How we manage disruption to work

2. How disruptions to work are managed will depend on whether they are known about in advance and reasonable action can be taken to manage their impact.

3. Disruptions may occur due to localised internet or cyber incidents that affect access to our systems, or disruptions which impact on the community as a whole, causing issues such as school closures or withdrawal of caring services, which may affect staff member's ability to attend work.

4. Where the disruption is known in advance, planning ahead can help manage the impact of exceptional disruption on individual's work commitments and their team. Staff members should be familiar with the Incident Response Plan in the event of exceptional disruption.

Planning ahead

5. Everyone should plan ahead and prepare for the potential impact of any exceptional disruption such as a localised internet or cyber incident; or alternative plans they may need to make, for example to meet their childcare and caring responsibilities.

6. Managers should:

   6.1. ensure that contingency plans are up-to-date;
   6.2. communicate plans to deal with any exceptional disruption event and the support available within their teams; and
   6.3. take individual circumstances into account, seeking advice from HR where necessary and apply our policies appropriately.

7. For planned disruption you should have had time to put in place suitable alternative plans and paid special leave and flexi adjustments will not be made.

Exceptional disruptions

8. Normal rules for requesting and taking all forms of leave continue to apply where there is an unplanned exceptional disruption to work. You should refer to the relevant leave policies for guidance:

SPSO%20-%20Leave.docx

9. This should last as long as is reasonably necessary to make suitable alternative arrangements. You should use other forms of leave if this takes longer than expected.

10. Managers should approve other leave only if they are satisfied:

    10.1. you have been unable to attend work because of the disruption; and / or
    10.2. a suitable alternative is not possible.

11. Where a flexi credit is appropriate, managers will be responsible for authorising them. When deciding on the flexi credit amount, managers should take into account the ability to work from home.

12. Sickness absence will not be treated as absence if it is as a direct result of the exceptional disruption.

Childcare and caring responsibilities

13. Exceptional disruption sometimes causes school closures or withdrawal of caring services. This may disrupt childcare or other caring responsibilities for some staff. It is expected that staff members will make every effort to arrange alternative care for a dependant, as in any emergency. The line manager should be informed if it is not possible to make alternative arrangements straightaway.

You should discuss using other leave, flexi-time and annual leave policies with your line manager to deal with a short-term emergency involving care of a dependant.

Back to the main Contents page

Incident Response Plan

Contents

Back to the main Contents page

Purpose and scope

1. The purpose of this Business Continuity Plan (BCP) is to minimise the impacts a business disruptive incident has on our ability to conduct our operations and maintain delivery of our essential functions and services.

2. The BCP documents the processes to be undertaken in the event of a business disruptive incident, failure or prolonged disruption affecting normal operations.

Critical business impact assessment

Critical business activity	Description	Critical?	Resources needed	Impact if not maintained	Time recovery objective
Emergency communications	Staff and contractor contact centre	Yes	• Call Chain Procedure arrangements • VOIP connection or emergency call centre	May not be able to sustain contact with staff for updates and instructions	Less than one hour
Information and Communication Technology (ICT) Systems	Access to essential ICT applications: • VOIP system • SCOTS Connect service • CMS	Yes	• contractor contact numbers and email addresses, as well as out of hours contacts (GBT; iTECS; CAS)	Ability to return to business as usual activities will be severely impeded	Within four hours
Governance	Provide medium-term recovery strategy, consider financial implications, manage external communication message	No	• one member of LT • mobile telephone coverage • internet access • SCOTS Connect service for email and non-casework information	Disjointed response, reputational damage	24 hours
External communications - website	Notification of the incident, the organisation response and alternative	No	• one member of Comms team • contractor • alternative host for website and social media	Disjointed response, reputational damage	24 hours

Critical business activity	Description	Critical?	Resources needed	Impact if not maintained	Time recovery objective
	arrangements for contacting the organisation.				
Minimum corporate services activities, including finance and HR	Staff personal data Payroll Access to bank account	Yes	• minimum of two available staff, one finance and one HR • internet access • VOIP connection with 0800 number working	May not be able to support staff with HR issues, or access personal data that may be required. May not be able to meet urgent financial requirements.	24 hours
Casework - SWF reviews	Respond to crisis grants reviews within 24 hrs	Yes	• minimum of two available staff • internet access • VOIP connection with 0800 number working • CMS application	Severe discomfort for members of the public	24 hours
Casework - First Contact	Respond to urgent enquiries, provide sign-posting services and manage the receipt of mail and email	No	• minimum of two available staff • internet access • VOIP connection with 0800 number working • CMS application	Serious implications for the performance measures of the complaints handling process. Minor annoyance for members of the public	One week
Casework - INWO complaints	Identify life-endangering reports within one week	No	• minimum one team member • internet access • VOIP connection with 0800 number working • CMS application	Possible high-risk situation resulting in loss of life	One week
Casework - Public Service Complaints (PSC)	Meet statutory requirements	No	• minimum six complaints reviewers • internet access • VOIP connection with 0800 number working	Implications for the performance measures of the business plan and	One month

Critical business activity	Description	Critical?	Resources needed	Impact if not maintained	Time recovery objective
			• CMS application • SCOTS Connect service for email and non-casework information	annoyance for members of the public	
Minimum facilities requirements, including mail and couriering activities	Locate an alternate premises for the receipt and dispatch of mail and couriered goods, and set up with requirements for effective processing.	No	• alternate location for processing mail • notification to Royal Mail and courier contractor • access to appropriate stationery for processing materials • multi-function device to scan material • internet access to inform staff of the receipt of mail	Implications for the accessibility of the SPSO to vulnerable groups and complaints handling process unable to access some vital paperwork	One month

Specific disaster and failure scenarios

3. Assumptions:

3.1. All staff have the facility to perform their duties from any networked environment using the provided SPSO laptops.

3.2. In extreme weather conditions, when the Scottish Government issues a red weather warning, all staff are expected to work from home and the building will remain closed. If an amber weather warning is issued, the minimum number of staff that could safely make it to the office to perform essential office-based duties would be expected to do so. Please also refer to the Met Office Weather Warnings Guide.

4. The four types of scenarios outlined below are:

4.1. reduced staff numbers;

4.2. reduced facilities / cyber incident;

4.3. security threat; and

4.4. body under jurisdiction suffering a catastrophic failure or major incident.

Incident scenario	Description	Actions
SPSO closed during normal work hours	General arrangements when the office is closed	When the SPSO is closed for business, the following arrangements are put in place: • 0800 SWF telephone lines would be diverted to an alternative telephone; • the usual closure announcements would be placed on the website, general email inboxes and the telephone messaging service; and • all staff would be responsible for ensuring their direct dial telephone numbers were to diverted to voicemail with an appropriate message recorded
Reduced staff numbers	Fifty percent staff reduction (pandemic or other impact)	If more than 50 percent of staff in any business area, or across the whole office, are not available and minimum cover arrangements cannot be met for more than one week. The Ombudsman will approve the reduction in performance and the appropriate stakeholder announcements will be made to this effect
Loss of key staff	Scheme of Delegation persons	If persons listed on the Scheme of Delegation were no longer available, this would stop decision-making impacting on the operations of the organisation. The SPCB would be notified immediately to provide emergency Accountable Officer / Ombudsman cover
Cyber incident	Loss of access to network and systems for more than one day	If the network provider confirmed that a reported problem was widespread across the network, all work would stop. The Ombudsman

Incident scenario	Description	Actions
		would request staff to work off-line to the best of their ability until the problem was rectified If staff are unable to access the secure network for more than one week, they will be asked to create a personal work email address for work use only. This is to reduce the risk of information leakage of organisation data, and a clear channel for internal organisation communications
Security threat	Threatening behaviour or terrorist threat	When a threat is received, the Leadership Team should be notified immediately. The Leadership Team member will inform all staff of the risk and the appropriate action to take. Please refer to the Bridgeside House Personal Safety document contained in the Bridgeside House Health, Safety and Security Handbook BH%20-%20Health %20Safety%20and%
Body Under Jurisdiction (BUJ) suffering catastrophic failure or major incident	If a Body Under Jurisdiction (BUJ) suffered a systems failure or physical disaster, there would be an impact on the SPSO's ability to meet its statutory duties, such as investigating complaints about the BUJ, how the BUJ is meeting the required Complaints Standards, implementing the SWF, or responding to an INWO report.	When notice is received that a BUJ's business has been compromised, the Leadership Team will liaise with the BUJ to identify the impact on SPSO activities and to discuss what arrangements the SPSO would need to put in place

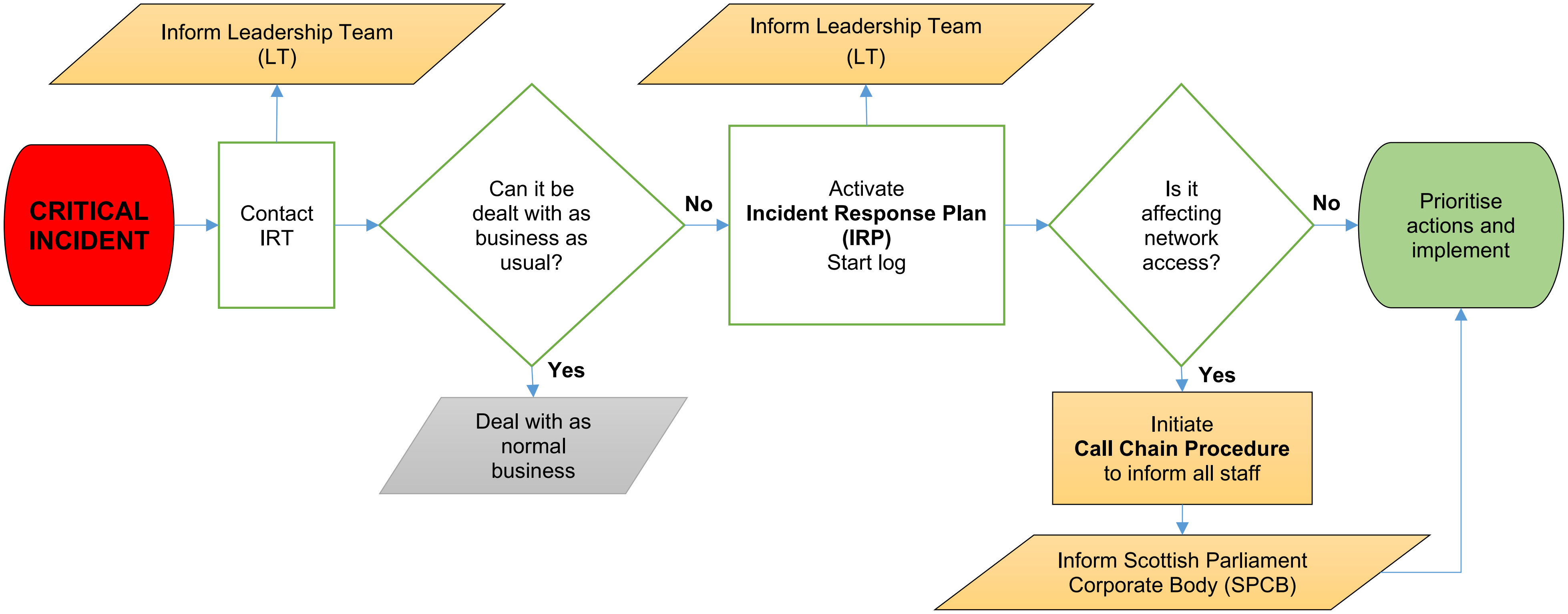
Incident scenario	Description	Actions
Reduced facilities	General arrangements when the building is closed	At any time the building is closed due to an incident, the following arrangements would be put in place: • signage would be added to the building and a note on the website explaining the problem; • mail and courier processes would be adjusted: **short-term:** Royal Mail and courier contractor would be notified to ensure mail pick-up was cancelled and mail delivery was held for the time period; **medium-term:** alternative location for the receipt and dispatch of mail and couriered material identified, Royal Mail and courier contractor informed of new address, machinery and stationery required for the process of mail would be set-up; • other contractors would be informed of the change of arrangements where required.
	Loss of Utilities (water, electricity, gas) to part or the whole building	If the problem persisted staff would be asked to work from home in the following circumstances: • loss of electricity supply for more than one hour; • loss of water supply to the whole SPSO location for more than four hours; and • loss of gas to the building for more than three days where the temperature dropped below the minimum statutory requirements. In the case of electricity, if initial enquiries identify that the problem could be rectified within an hour, staff would be asked to take a break away from the office and return after an allotted period

Incident scenario	Description	Actions
	Evacuation followed by denial of access to building	The Ombudsman would approve the IRT to ensure the provision of essential provisions to maintain the health and safety of all staff, provide communications channels for staff to contact friends or family and arrange transport home where required. Selected members of staff have corporate credit cards to facilitate this

Activation of the plan

5. Any two members of the IRT can agree to activate the Plan. They will confirm activation to all other IRT and Leadership team members. Once the Plan is in operation, the IRT will follow the procedures contained in the Plan. The IRT Manager will confirm when the Plan is deactivated.

6. During the period when the Plan is in operation, all staff must follow the instructions of the IRT and must avoid taking any unilateral action that may hamper or jeopardise recovery.


Inform Leadership Team (LT)
Inform Leadership Team (LT)
CRITICAL INCIDENT
Contact IRT
Can it be dealt with as business as usual?
No
Yes
Activate **Incident Response Plan (IRP)** Start log
Is it affecting network access?
No
Yes
Prioritise actions and implement
Deal with as normal business
Initiate **Call Chain Procedure** to inform all staff
Inform Scottish Parliament Corporate Body (SPCB)

Staff notification of critical incident

Responsibilities

7. IRT will test this procedure annually and report the results to the Leadership Team.

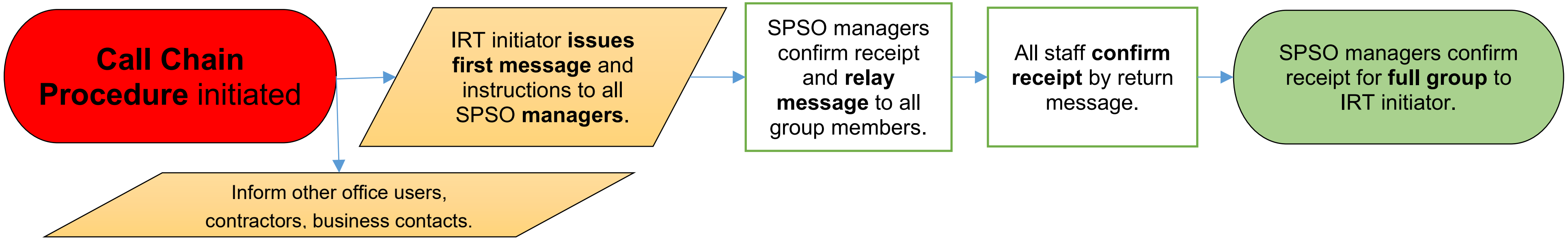
8. Leadership Team must ensure one member is contactable at all times.

9. Managers must be able to contact their team members at any time and are responsible to maintain current contact details for all member of their group, at minimum a telephone number and personal email address; and regularly test these contact details.

   9.1. Managers will avoid using group messaging applications to contact staff members. This will avoid unnecessary traffic on personal devices out-of-hours. Instead, managers will use a text / message broadcasting method, using a social media application to minimise disruption. If the manager or a staff member does not use this application, the manager will agree the preferred and most effective out-of-office contact method with group members.

Procedure

10. The Call Chain Procedure will be initiated by a member of the IRT.


Call Chain Procedure initiated
IRT initiator **issues first message** and instructions to all SPSO **managers**.
SPSO managers confirm receipt and **relay message** to all group members.
All staff **confirm receipt** by return message.
SPSO managers confirm receipt for **full group** to IRT initiator.
Inform other office users, contractors, business contacts.

11. If required, any further information or instructions will be issued to line managers by the Human Resources officer, including an emergency contact number for staff and their relatives.

Critical incident log

12. For critical incidents, when a normal incident log is not appropriate, a real-time Critical Incident Log should be adopted and maintained by a nominated staff member, who is not part of the IRT, to record all decisions and actions taken during the incident. The completed logs will provide a source of data for subsequent analysis and management information.

13. The log will be used:

    13.1. as an accurate record of who, what, when, where and how;
    13.2. to record in real time key information, including timings, contacts, and details of key decisions;
    13.3. to handover to the emergency response teams, or others, if required;
    13.4. to debrief an incident;
    13.5. as a record of a major incident for future reference; and
    13.6. for reference by major stakeholders and legal bodies.

Example log information

Loggist Name:

Sheet No.x - Title

Date	Time	Event (meeting, call, activity)	Action / Decision Taken	Who

Critical incident communications arrangements

14. A serious incident affecting the SPSO may attract interest from local and national media. This section of the plan outlines how it would be handled by the Engagement and Communications Manager who will assemble an appropriate team to assist.

Key points

15. Only the Ombudsman and Engagement and Communications Manager may liaise with the media when the Incident Response Plan is activated. Other members of the leadership team may deputise when required.

16. All staff are required to refer media interest to the nominated media co-ordinators, either the Ombudsman and/or Engagement and Communications Manager.

17. Staff are not to comment on the incident publicly, for example, on social media.

18. The Engagement and Communications Manager must be kept informed at all times of actions being taken by other IRT members.

19. Telephone facilities to establish a response centre will be made available through our contracted telephony provider.

20. A draft outline initial press statement is outlined below.

21. A list of key media contacts is here.

22. Service users must be kept up-to-date about our services' availability through the available channels, in the first instance website and social media.

Communication principles

23. If the critical incident involves an accident or other risk to health, staff and the concerns of their relatives will take priority. Local media can play a valuable role in providing reassuring information.

24. During the period that the IRP is activated, the Engagement and Communications Manager will:

    24.1. keep all lines of communication clear and ensure all personnel dealing with the media have the same information;
    24.2. refuse to comment on what has happened until the information has been verified by the emergency services;
    24.3. be positive and available when dealing with press and media enquiries;
    24.4. log all media calls; and
    24.5. give all the media the same information and tell them when new information will be available.

Media communications considerations

25. The considerations are:

    25.1. ABC – Acknowledge, Bridge, Comment;
    25.2. PPP – Praise, Pity, Pledge;
    25.3. develop in three stages to match journalist's style: what has happened, the context and a look forward;

25.4. speed of reply is essential as false information can spread very quickly through social media;

25.5. the public want information that is of benefit to them and allows them to take control – they will only do this if they trust the person who is providing that information;

25.6. openness and honesty are essential ingredients for building trust and empathy. It is vital to maintain that trust;

25.7. tell people what is known and then tell them what you are doing to find out what is not known; and

25.8. provide proof points and evidence to support arguments: pictures can help this process, especially for foreign audiences where English is not their first language.

26. Typical media questions may include:

26.1. What happened?

26.2. Why did it happen?

26.3. Who is to blame?

26.4. Was this an accident waiting to happen?

26.5. How many people are affected?

26.6. Are the public at risk?

26.7. When was it discovered?

26.8. What are you doing about it?

Draft outline initial press statement

27. The following draft is to ensure each topic is addressed and will be updated in the light of the specific circumstances.

Statement following incident at the SPSO Edinburgh on (Date / Time)

28. At (time) today (date) (emergency appliances) attended an incident at the office of the SPSO at 99 McDonald Road, Edinburgh.

29. We are working to restore services to the public and other stakeholders as soon as possible at the organisation's alternative site (address).

30. The following statement provides up-to-date information on the circumstances.

Personal Safety

31. SPSO staff and relatives seeking information should contact our emergency helpline on [xxx].

32. Staff not currently involved in implementing our Incident Response Plan have been sent home.

33. The site is currently only accessible by emergency services.

Damage to property

34. We anticipate that access to the building should be possible from (date) to obtain records and full work will be possible from (date).

Effect on business

35. We are working to ensure that service will be restored as soon as possible.

36. Our Incident Response Plan involves key staff using the organisation's alternative location in Edinburgh.

37. Most services will be unaffected by the incident, although outside contact may limited today.

38. A helpline for the public is available on the main reception telephone line at [enter location and number].

Cyber Security Incident

39. [On X date] SPSO was the victim of a cyber security attack.

40. While we are still investigating the full extent of the attack, we [do not] believe that private personal data has been accessed.

41. We are working with the police, cyber security experts and the Scottish Government to understand the full extent of the attack and will be providing an update as soon as we have more information.

42. Where we find that identifiable personal data has been accessed, we will contact those affected directly.

43. We ask those who have used our service over the last five years to be extra vigilant of potential scam calls and emails over the coming weeks.

44. We recognise people will be concerned, but ask that you wait for us to contact you or have emergency contact details in place.

45. We apologise for the distress and inconvenience this may cause.

46. We are committed to providing regular updates as more information becomes available.

47. Over the next week we will be operating a reduced level of service.

Further Information

48. For further information, contact: [xx] Engagement and Communications Manager (cover - Ombudsman)

Post incident

Debrief

49. The IRT Director should ensure a post-incident debrief is held within two weeks of an incident being closed and normal operations have resumed. The following people will be invited to the debrief:

    49.1. Plan Owner;
    49.2. Incident Management Team;
    49.3. Representatives from impacted areas; and
    49.4. Review lead.

Review

50. A review lead will be appointed to lead on a review of the incident. The purpose of the review is to:

    50.1. Investigate / confirm the cause(s) of the incident;
    50.2. consider possible mitigations to reduce impact of future incidents of a similar nature;
    50.3. assess the initial response to the incident;
    50.4. assess the effectiveness of continuity measures;
    50.5. assess the effectiveness of communication;
    50.6. assess the effectiveness of the management response and IMT; and
    50.7. identify improvements

Post incident report and action plan

51. Identified improvements will be formed into specific actions with an action owner and a deadline.

52. The report and action plan will be discussed regularly at Leadership Team level.