Business Continuity

Only the Leadership Team 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

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 hrs	24 hrs	48 hrs	1 wk	2 wks	4 wks
Emergency Comms – call tree							
ICT Systems – VOIP, CMS, SCOTS network							
Governance							
External Comms – website							
Casework Management System (CMS) – SWF							
Casework Management System – First Contact							
Casework Management System (CMS) - INWO							
Casework Management System (CMS) - PSC							
Corporate Services – Finance, HR							
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 impacts all areas of the organisation. The loss becomes more critical the longer it continues from 24 hours downtime. If it continues for more than two-weeks, the whole organisation will be in a severe situation with potential long-term effects. One month without CMS and SCOTS Connect service would critically threaten the SPSO's ability to carry out its statutory 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. two working weeks without CMS access may impede the reporting of life-endangering actions through Independent National Whistleblowing Officer (INWO);

7.5. one month without CMS access may have serious implications for the investigations into public sector complaints (PSC); 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.

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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.

8.5. 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.

8.6. 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.


GBT Disaster Recovery Agreement


GB TECHNOLOGIES LTD BCP.docx

8.7. 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.

8.8. The CMS has 24/7 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 Disaster Recovery v1.2.pdf

8.9. 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.

8.9.1. 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.

8.9.2. The Recovery Point Objective would be the previous night's backup. Potentially, the worst case would be the loss of one working-days' material, should an incident occur at the end of a full working day requiring a restore from the previous night's backup.

8.9.3. The last three days of overnight backups are stored in an encrypted format and disconnected from the platform. The recovery of SPSO backups is tested by the CMS supplier annually.

8.10. 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

8.11. 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

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

9.1. 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.

9.2. 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.

9.3. 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:

9.3.1. one Leadership Team member;
9.3.2. two Scottish Welfare Fund members;
9.3.3. two Assessment and Guidance members;
9.3.4. six Complaints Reviewers;
9.3.5. one Independent National Whistle-blowing Officer member;
9.3.6. one Corporate Service member;
9.3.7. one Improvement, Standards and Engagement member; and
9.3.8. with management provided by three line managers who may be included in the above numbers, one of which is a casework manager.

Incident Response Team (IRT)

10. The IRT is responsible for providing overall direction of the incident recovery operations. It must ascertain the extent of the problem or damage, activate the Plan if required, monitor and report recovery progress. Specific responsibilities include:

10.1. evaluation of the extent of the problem and the potential consequences;
10.2. initiating business continuity procedures;
10.3. activation and deactivation of the Plan;
10.4. liaising with emergency services;
10.5. maintaining external public relations;
10.6. monitoring recovery and assuring achievement of the Plan;
10.7. ensuring maintenance of security; and
10.8. monitoring control of emergency expenditure.

Testing and Maintaining the Plan

BCP annual checklist - template.

11. 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.

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

    12.1. testing the Call Chain Procedure annually;
    12.2. testing written procedures to re-establish ICT systems, such as the telephone system after a power-cut, by non-trained staff; and
    12.3. reviewing emergency contact details each year and updating where necessary.

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

Back to the main Contents page

Incident Response Plan

Contents

Back to the main Contents page

Roles and Responsibilities

1. 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	Description	Areas of Responsibility
Gold Strategic	**Leadership Team (LT)**	• Ombudsman • Director • Head of Improvement, Standards and Engagement	**Hand off** – overall view of the incident, provide leadership, commitment and resources as part of governance	• 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)**	• Corporate Services Manager (IRT Manager) • ICT Systems Analyst (Deputy IRT Manager) • Building Coordinator (Deputy IRT Manager) • Communications and Engagement Manager • HR Manager • Head of Investigations	**Hands in** – respond to incident, how to coordinate the response. Directing the operations level and working towards the strategic objectives	• 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 • Human Resources and internal communications - staff welfare

Level	Role	Members	Description	Areas of Responsibility
				• 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**	• Corporate Services Team members • Comms Team members • Managers and Team Assistants • other staff members as required	**Hands on** – doing the response on the ground	• 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

Strategic 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 arrangements for contacting the organisation.	No	• one member of Comms team • contractor • alternative host for website	Disjointed response, reputational damage	24 hours
Casework - SWF reviews	Respond to crisis grants reviews within 24 hrs	Yes	• minimum of two available staff • internet access	Severe discomfort for members of the public	24 hours

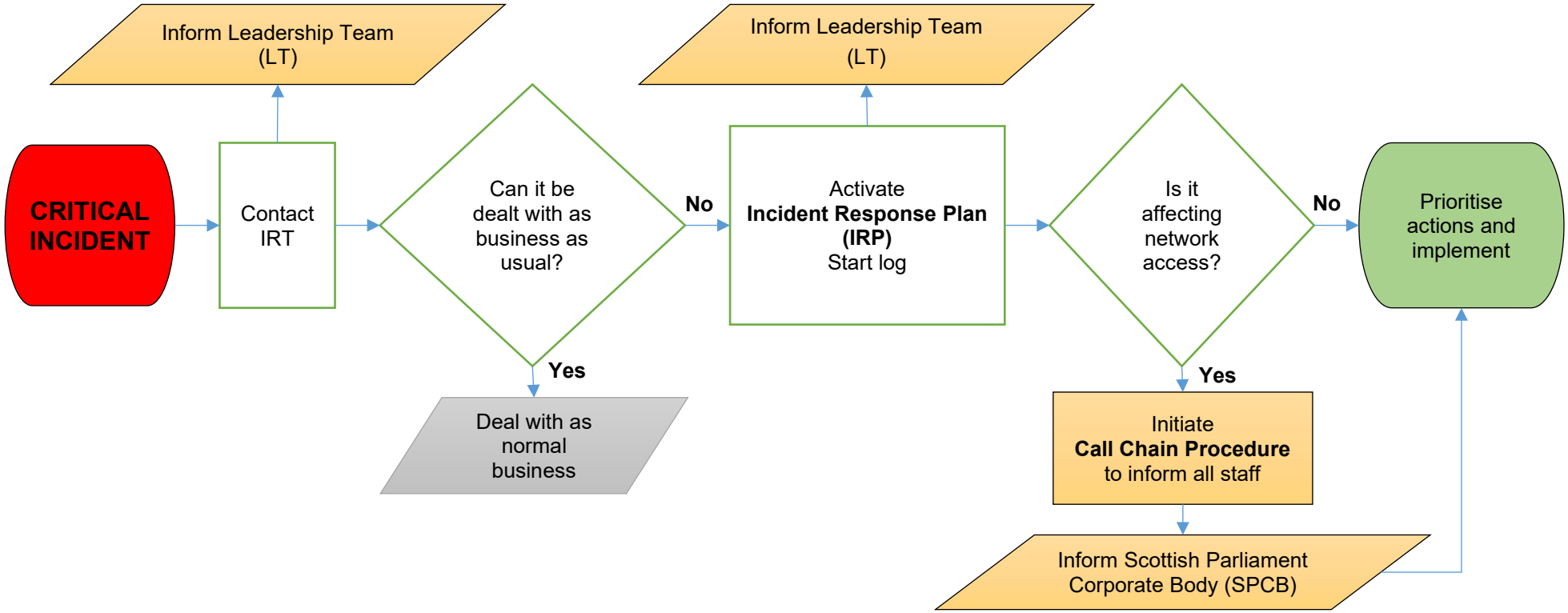
Critical Business Activity	Description	Critical ?	Resources needed	Impact if not maintained	Time recovery objective.
			• VOIP connection with 0800 number working • CMS application		
Casework - First Contact	Respond to urgent enquiries, provide sign-posting services and manage the receipt of mail and 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	Two weeks
Emergency repairs and maintenance for utilities	Priority contractor contacts to provide emergency repairs and restore services	No	• contractor contact numbers and email addresses	Response to incident may be slowed, potentially dangerous situations may not be remedied	Two weeks
Minimum business as usual activities, including Casework - Public Service Complaints (PSC)	Meet statutory requirements	No	• minimum staff across all areas of the business • internet access • VOIP connection with 0800 number working • CMS application • SCOTS Connect service for email and non-casework information	Implications for the performance measures of the business plan and annoyance for members of the public	One month

Critical Business Activity	Description	Critical ?	Resources needed	Impact if not maintained	Time recovery objective.
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

Activation of the Plan

2. 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.

3. 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.



Staff Notification of Critical Incident

Responsibilities

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

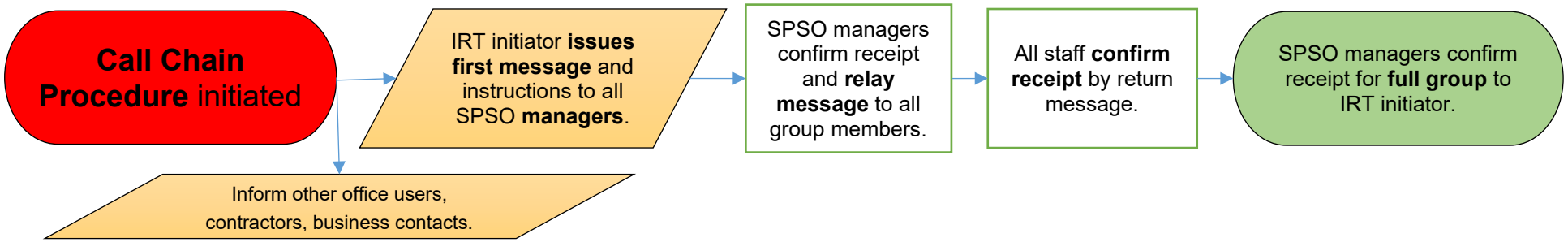
5. Leadership Team must ensure one member is contactable at all times.

6. 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.

    6.1. 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 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

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



8. 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.

IRT Specific Responsibilities during a Critical Incident

9. The IRT is responsible for providing overall direction of the incident recovery operations. It must ascertain the extent of the problem or damage, activate the Plan if required, monitor and report recovery progress.

IRT Manager (Corporate Services Manager)

Deputy: Director

10. Take overall responsibility for management, control and activation of the Plan.

11. 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.

12. Actions are:

    12.1. initiating the call chain procedure;
    12.2. identifying support staff to assist with incident response; and
    12.3. contacting contractors.

Deputy IRT Manager (ICT Systems Analyst and Building Coordinator)

Deputy: Team Assistant – ICT and Finance

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

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

14. Actions are:

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

        14.2.1. establish procedures and schedules for the operation of standby facilities;
        14.2.2. install operating systems, application software and data on standby and replacement IT facilities;

14.2.3. retrieve documentation and media from backup storage;
14.2.4. implement interim processing and backup procedures;
14.2.5. enforce logical security at the standby site;
14.2.6. initialise and test standby hardware, operating systems and communications;
14.2.7. contact suppliers and order and configure replacement facilities; damage evaluation, identification of salvage, removal of re-usable equipment;
14.2.8. provide information and support for interim IT facilities; and
14.2.9. reconfigure the communications network as required and monitor performance.

Communications and Engagement Manager

Deputy: Ombudsman

15. 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.

16. Actions are:

16.1. ensuring a response centre telephone facilities are set up;
16.2. drafting press statement and communicating with media;
16.3. updating SPSO website and social media with statement to service users/the public;
16.4. monitoring media and social media;
16.5. logging all media calls; and
16.6. ensuring staff know that media enquiries are directed to Communications and Engagement Manager.

HR Officer

Deputy: Director

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

18. Actions are:

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

Building Coordinator

Deputy: Corporate Services Officer

19. 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.

20. Actions are:

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

Head of Investigations

Deputy: Casework Manager

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

22. Actions are:

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

Critical Incident Log

23. 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.

24. The log will be used:

    24.1. as an accurate record of who, what, when, where and how;
    24.2. to record in real time key information, including timings, contacts, and details of key decisions;

24.3. to handover to the emergency response teams, or others, if required;
24.4. to debrief an incident;
24.5. as a record of a major incident for future reference; and
24.6. 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

25. 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

26. Only the Leadership Team and Engagement and Communications Manager may liaise with the media when the Incident Response Plan is activated.

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

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

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

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

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

32. A list of key media contacts is here.

33. 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

34. 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.

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

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

Media Communications Considerations

36. The considerations are:

    36.1. ABC – Acknowledge, Bridge, Comment;
    36.2. PPP – Praise, Pity, Pledge;
    36.3. develop in three stages to match journalist's style: what has happened, the context and a look forward;
    36.4. speed of reply is essential as false information can spread very quickly through social media;
    36.5. 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;
    36.6. openness and honesty are essential ingredients for building trust and empathy. It is vital to maintain that trust;
    36.7. tell people what is known and then tell them what you are doing to find out what is not known; and
    36.8. provide proof points and evidence to support arguments: pictures can help this process, especially for foreign audiences where English is not their first language.

37. Typical media questions may include:

37.1. What happened?
37.2. Why did it happen?
37.3. Who is to blame?
37.4. Was this an accident waiting to happen?
37.5. How many people are affected?
37.6. Are the public at risk?
37.7. When was it discovered?
37.8. What are you doing about it?

Draft Outline Initial Press Statement

38. 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)

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

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

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

Personal Safety

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

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

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

Damage to property

45. 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

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

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

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

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

Further Information

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

Specific Disaster and Failure Scenarios

51. Assumptions:

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

    51.2. 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.

52. The four types of scenarios outlined below are:

    52.1. reduced staff numbers;
    52.2. reduced facilities / cyber incident;
    52.3. security threat; and
    52.4. body under jurisdiction suffering a catastrophic failure or major incident.

Reduced staff numbers

Fifty percent staff reduction (pandemic or other impact)

53. If more than 50 percent of staff 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

54. If persons listed on the Scheme of Delegation were no longer available, the SPCB would be notified immediately to provide emergency Accountable Officer cover.

Reduced facilities / cyber incident

Loss of access to network and systems for more than one day

55. If the network provider confirmed that a reported problem was widespread across the network, the Ombudsman would request staff to work off-line to the best of their ability until the problem was rectified.

56. 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.

57. iTECS mitigating plans and BCP arrangements.

iTECS Resilience.docx

General arrangements when the building or office is closed

58. At any time the building is closed due to an incident, the following arrangements would be put in place:

    58.1. signage would be added to the building and a note on the website explaining the problem;

    58.2. mail and courier processes would be adjusted:
        58.2.1. 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; and
        58.2.2. 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;

    58.3. other contractors would be informed of the change of arrangements where required.

59. When the SPSO is closed for business, the following arrangements are put in place:

    59.1. 0800 SWF telephone lines would be diverted to an alternative telephone;
    59.2. the usual closure announcements would be placed on the website, general email inboxes and the telephone messaging service; and

59.3. all staff would be responsible for ensuring their direct dial telephone numbers were to diverted to voicemail with an appropriate message recorded.

Loss of Utilities (water, electricity, gas) to part or the whole building

60. 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.

61. If the problem persisted staff would be asked to work from home in the following circumstances:

61.1. loss of electricity supply for more than one hour;
61.2. loss of water supply to the whole SPSO location for more than four hours; and
61.3. loss of gas to the building for more than three days in wintery conditions.

Evacuation followed by denial of access to building

62. 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.

Security threat

Threatening behaviour or terrorist threat

63. 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.

Body Under Jurisdiction suffering a catastrophic failure or major incident

64. 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.

Annex 1: IRT Critical Contact Details (Confidential not for publishing)

Incident Response Team

Title	Name	Work mobile	Personal Mobile
Corporate Services Manager (IRT Manager)			
ICT Systems Analyst (IRT Deputy Manager)			
BH Building Coordinator			
Communications and Engagement Manager			
HR Manager			
Head of Investigations			

Leadership Team

Ombudsman		
Director		
Head of ISE		

Main key holder contact details

Mitie Security Key holder Services	
Corporate Services Manager	

Emergency business contacts - Priority A

Service	Company / Contact	Telephone No	Contract / Account Number
Alarm system	IMMS	0131 664 5052	SPSO – Bridgeside House
Building Contents Insurance	Hiscox	0131 225 7777	**Policy:** PL-PSC04001287044/03
Casework Application	CAS – Workpro - Simon Laxton (Business Relationship Manager)	0131 449 7071 / 07541 206 996	SPSO
	CAS – Workpro – Marc Forrest (Infrastructure Manager)	0131 297 2117 / 07507 89 22 39	
	CAS – Workpro – main line	0131 297 2141	
H&S Competent Person	Worknest (UK) Ltd Roxanne Delaro (H&S Consultant)	0345 226 8393 (24 hour advice line) 07850 646849	Scottish Public Services Ombudsman

Service	Company / Contact	Telephone No	Contract / Account Number
IT Network provider	SCOTS – IT Server and Hardware	0131 244 8500 (day time)	SPSO
Key holder	Mitie Security	01908 671317	SPSO – Bridegside House
Landlord	C&W Assets	0131 336 2181	Bridgeside House
Scottish Parliament Corporate Body	SPCB office-holder	0131 348 6851	
Telephony provider	GB Technologies	01896 752 607	GBT 00831

Emergency business contacts - Priority B

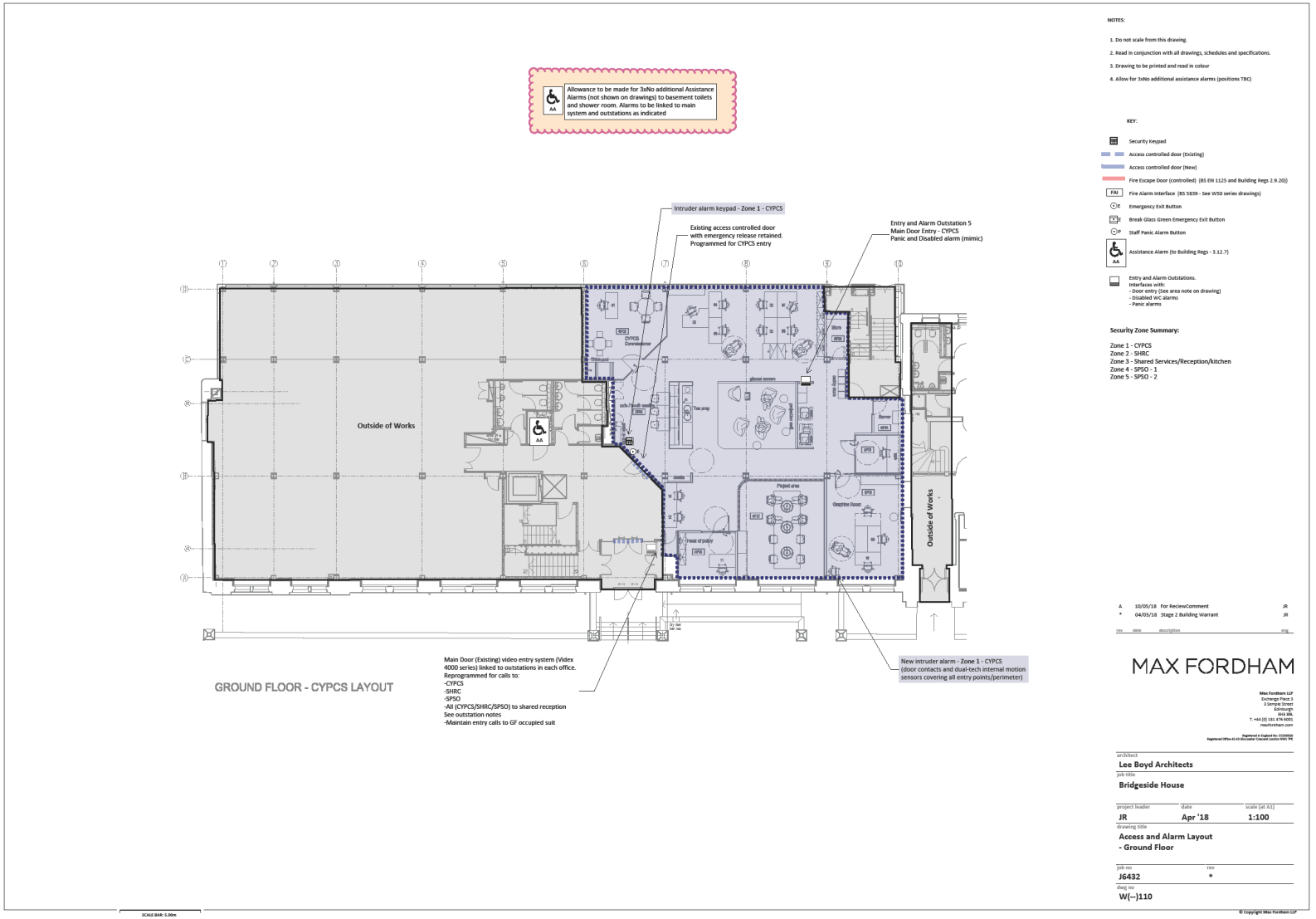
Service	Company / Contact	Telephone No	Contract / Account Number
Cleaners	Mitie Cleaning	07368601044	SPSO
Waste and Recycling management	Change Waste	0800 694 0158 0131 555 4010	PC 10430
	Paper Shredding Services	0141 440 1515	SPSO
Mail collection and delivery services	Eagle Couriers	0845 123 1230	PS 6408
	Franking Machine – Lease CF corporate Franking Machine – Northern Services Franking Machine – Pitney Bowes	0800 756 0827 01355 241 333 08444 992 992	C203193/W S504 14037931
	Royal Mail – Collection Service	0131 458 8644	
	Royal Mail – Deliveries	03457 740 740 customer service	
Utilities	Clear Business - Water	08456 028 855	2392938
	Total Gas and Power	01737 275 501	3001130231

Media Contacts

The media co-ordinator should consider contacting the following with any media statement.

Outlet	Email	Office telephone / mobile	Twitter
BBC TV Scotland	scottish.planning@bbc.co.uk	0131 557 5888	@BBCScotlandNews
STV	news@stv.tv	0131 200 8000/ 0141 300 3000	@STVNews
BBC Radio Scotland	scottish.planning@bbc.co.uk		@BBCRadioScot
Forth 1	news@radioforth.com	0131 557 1005	@forthone
The Herald / Sunday Herald	news@theherald.co.uk	0141 302 7000	@heraldscotland
The Scotsman / Scotland on Sunday	newsdeskts@scotsman.com	0131 311 7311	@TheScotsman
Edinburgh Evening News	newsen@edinburghnews.com	0131 311 7311	@edinburghpaper
The Daily Mail in Scotland	scotland@dailymail.co.uk		@MailOnline
Scottish Daily Record	reporters@dailyrecord.co.uk	0141 309 3251	@Daily_Record
Metro	webnews@metro.co.uk	020 3615 0000	
The Daily Telegraph (Edinburgh office)	media.enquiries@telegraph.co.uk		@Telegraph
Holyrood Magazine	Mandy@holyrood.com	0131 285 1605	@HolyroodDaily
The Times	home.news@thetimes.co.uk	0141 420 5100	@thetimes
Sunday Times Scotland	newsdesk@sunday-times.co.uk		@thetimes
Sunday Mail	reporters@sundaymail.co.uk	0141 309 3232 / 0141 309 3251	@Sunday_Mail

Annex 2: Bridgeside House Floor Plans



Link to SPSO seating plan: FloorPlanMASTER.xlsx

Annex 3: ICT System Document

Link to documents:

- CAS Workpro ICT System Documentation – Architecture v2.1 : 20200614 Workpro System Documentation - Architecture (A31175333)
- CAS Workpro ICT System Documentation – v3.6 (June 2019) - 20200614 Workpro System Documentation v2-3(2016Format)-CAS (A31175344)
- CAS Workpro Escrow Agreement (Dec 2020) - 160616 Workpro ESCROW Agreement (A31198246)
- CAS Workpro Disaster Recovery – 210331 Technical Notes for Private Cloud Customers
- CAS Workpro Disaster Recovery – 210331 v.1.2

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.

Childcare and caring responsibilities

5. 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.

6. There may be other leave available to deal with a short-term emergency. This will last as long as is reasonably necessary to put in place suitable alternative care arrangements.

7. Other forms of leave can be used if you need a longer period away from work.

How our leave policies apply

8. 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. The following guidance applies in event of exceptional disruptions only.

Annual leave, flexi leave, other leave

9. Link to the Leave handbook.

10. Normal rules for requesting and taking all forms of leave continue to apply where there is an unplanned exceptional disruption to work. Your manager may be able to grant you other leave if your childcare or other caring responsibilities are affected.

11. 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.

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

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

13. 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.

14. You should get flexi credit for all authorised hours worked if you are able to work from home. You will also be given flexi credit in the event of office closure.

Absence

15. Your absence will not be treated as absence if it is as a direct result of exceptional disruption and caused by your caring responsibilities.

Planning ahead

16. 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.

17. Managers should:

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