

The Highland Council
Resources Committee – 27 May 2015

Agenda Item	16
Report No	RES/43/15

Corporate Development Service's Business Continuity Plan (BCP)

Report by Depute Chief Executive/Director Corporate Development

Summary

This report introduces the attached Corporate Development Service's Business Continuity Plan (BCP). This plan identifies key business activities delivered by the Service. It has been prepared according to a methodology agreed by the Executive Leadership Team which identifies key activities which must be maintained against a range of timeframes. Once the Service's BCP is formally adopted, it becomes an integral part of the Council's overall General BCP. Training for staff in the activation of the BCP will follow, as will testing and periodic (annual) review.

1. Background

- 1.1 The Corporate Development Service's BCP has been drawn up in response to the requirements of the Civil Contingencies Act as well as it being good business practice. It seeks to identify how key activities will continue to be delivered during a major incident.
- 1.2 Key business activities were identified by a working group of Service managers who, using a risk matrix, identified and assessed the likelihood and impact of the loss of these activities. The risk scoring which followed allowed the team to rank these risks and to prepare specific arrangements to mitigate them.

2. Approach

- 2.1 As agreed by the Executive Leadership Team, the approach throughout has been to concentrate on consequences rather than trigger events, i.e. dealing with overall impacts rather than concentrating on a wide range of scenarios; for instance, key activities could be affected by a range of events that cause loss of staff (e.g. widespread illness, industrial action, severe weather) but loss of staff remains the outcome.
- 2.2 BCP has been a new activity for some managers and there was a need to assist the working group, particularly in carrying out a business impact analysis. This element of the approach is fundamental in identifying those key areas which are priorities for the business.

3. Monitoring and Performance Reporting

3.1 Progress in further development of the BCP will be monitored periodically by the Executive Leadership Team at no more than a quarterly interval and by Internal Audit at no more than an annual basis.

3.2 Once the Service's BCP is adopted, it becomes an integral part of the Council's overall General BCP. This overall General BCP will be presented to committee when all Service's BCPs are adopted.

4. Implications

4.1 There are no Financial, Equalities, Rural or Carbon Clever impacts arising as a direct result of this report.

4.2 Resource and Risk implications are noted throughout the BCP itself.

4.3 There is a follow-on time commitment required to meet training and exercising needs as the BCP is further developed.

Recommendation

The Resources Committee is asked to:

- a) Approve the Corporate Development Service's Business Continuity Plan.

Designation: Depute Chief Executive & Director Corporate Development

Date: 6 May 2015

Author:

Attachments: Service BCP - Corporate Development

THE HIGHLAND COUNCIL

SERVICE BUSINESS CONTINUITY PLAN FOR CORPORATE DEVELOPMENT

BC Plan Owner: Michelle Morris, Depute Chief Executive & Director Corporate Development

Release Date: 06-05-2015

Review Date: 01-10-2015

Document Version: 0.2

DISTRIBUTION LIST (to assist in updating and revising the plan, an up-to-date list of all plan holders and persons supplied with a copy of the plan should be included)

Copy Number	Name	Location
	Corporate Development Senior Management Team	HQ
	Digital Transformation	HQ
	Customer Services	HQ
	ICT Services	HQ

REFERENCES AND RELATED DOCUMENTS

<u>Document Titles</u>
Fujitsu ICT Contract; Vodafone Pathfinder North Contract; SWAN Contract
THC_BCDR_Plan-v2; Customer Services Service Centre Business Continuity Plan v1.1
National Records of Scotland (NRS) Civil Emergency Procedures (2013); NRS Instructions to Registrars in the event of a Disaster in a Registration Office.

AMENDMENT LIST

Amendment Number	Reason for Amendment	By Whom
0.1	First draft	T Brown, ICT Service Officer
0.2	General review	T Brown, ICT Service Officer Process Owners
0.3	General review – 6 th May 2015	Corporate Development Senior Management
1.0	Final document – 6 th May 2015	Corporate Development Service – SMT

SERVICE BUSINESS CONTINUITY PLAN

1. **AIM.** The aim of the Service Business Continuity Plan (BCP) is to maintain the delivery of key services within critical business areas in the event of a major incident.
2. **OBJECTIVES.** The BCP has several inter-related objectives, namely to;
 - Identify and prioritise critical business areas,
 - Complete a business impact analysis,
 - Identify where mitigatory actions or risk reduction can be applied,
 - Detail the immediate response to a major incident, and
 - Review and update the plan on a regular basis or in light of a real incident.
3. **CONSEQUENCES.** The Service BCP identifies the actions required to deal with a range of risks to a number of identified critical business areas. These risks have been identified on the basis of consequences rather than trigger events since, for instance, “loss of staff” can arise from a number of different triggers (e.g. industrial action, illness, severe weather). The BCP therefore focusses on consequence management.
4. **CRITICAL BUSINESS AREAS.** Critical business areas have been identified through conducting a Business Impact Analysis (BIA) for the Service. The BIA is an integral part of the Service BC Plan since it identifies the relative importance of each critical business area and also ranks these on the basis of those critical business areas which;
 - Must be kept functioning 24/7 if immediate serious consequences are to be avoided,
 - Could accept a business interruption of up to 3 days before having serious consequences, and
 - Could accept a business interruption of up to 7 days before having serious consequences.
5. **ACTION PLANNING.** The BIA also assesses the likelihood of any particular risk occurring and ranks the risk accordingly. A series of action plans, for dealing with each of these risks to the delivery of critical services and activities, is required. Two templates for these individual action plans are shown below as partly-worked examples. These templates can be adapted as required, as long as the information provides clear links to the measures and arrangements identified.

CORPORATE DEVELOPMENT SERVICE - BUSINESS IMPACT ANALYSIS (BIA) TABLE

Risk Number	Critical Business Area	Loss of Staff	Loss of Buildings	Loss of Communications	Loss of ICT	Loss of Internet	Loss of Utilities	Loss of Internal Suppliers	Loss of External Suppliers	Excess Demand	Loss of Critical or Sensitive Data	Loss of Reputation	Loss of Compliance and/or Accreditation	Risk Owner
		a.	b.	c.	d.	e.	f.	g.	h.	i.	j.	k.	l.	
24/7														
CD 01	Provision of Internet Service	N	N	Y	Y 4,4=16	Y	Y 4,3=12	N	Y 4,4=16	N	N	Y	N	Vicki Nairn
CD 02	Provision of Service Centre	Y 4,4=16	Y 2,4=8	Y	Y 4,4=16	Y	Y 4,4=16	N	Y 4,4=16	Y 4,5=20	Y 3,4=12	Y	N	Vicki Nairn
CD 03	Provision of WAN and LAN		Y 4,4=16		Y 4,4=16		Y 4,4=16		Y 4,4=16				Y 4,4=16	
CD 04	Deaths Registration	Y 1,2=2	N	Y	N	N	Y 4,1=4	N	N	Y 3,4=12	Y 3,4=12	Y	Y 1,4=4	Vicki Nairn
Up To 3 Days														
CD 05	CRM System	Y 4,2=8	N	Y	Y 4,2=8	Y	Y 4,1=4	N	Y 4,2=8	N	N	N	N	Vicki Nairn
CD 06	Provision of HR Service	Y 1,2=2	N	N	Y 4,2=8	N	Y 4,1=4	N	N	N	Y 3,4=12	N	N	John Batchelor
CD 07	Access to Critical Data	N	N	Y	Y 4,4=16	N	Y 4,4=16	N	Y 4,4=16	N	Y 3,4=12	N	N	Michelle Morris
CD 08	Provision of Legal Services	Y 1,2=2	N	Y	Y 4,2=8	Y	Y 4,1=4	N	N	N	Y 3,4=12	Y	N	Stewart Fraser
Up To 7 Days														
	None Identified													

CRITICAL BUSINESS AREA					
24/7					
CD 01 Provision of Internet Service	Risk Number as listed in the BIA	Risk Rating taken from the BIA	Risk description as listed in the General BCP	Description of preventative or mitigatory measures. Where these are not in place, they must be addressed in an appropriate action plan.	Description of contingency arrangements. Where these are not in place, they must be addressed in an appropriate action plan.
	CD-01d	16	Loss of ICT	<ul style="list-style-type: none"> Contractual break/fix arrangements for the ICT Contract (schedule 8), PfN contract (part 2.2) and Jadu contract (SLA Matrix) for short term losses. Contractual Disaster Recover/ Business Continuity arrangements - ICT Contract (schedule 9) and PfN contract (part 7.6) for long term losses. SSE failover between Mountain and East Coast trunk routes. Agreed breakout arrangements. 	<ul style="list-style-type: none"> Manual activation of Jadu failover to Disaster Recovery site. Agreed ICT Business Continuity plan in place.
	CD-01f	12	Loss of Utilities	<ul style="list-style-type: none"> Re-route of internet traffic through Nevis House if experiencing power issues at HQ. Agreed breakout arrangements. 	
	CD-01h	16	Loss of External Suppliers	<ul style="list-style-type: none"> As part of Procurement and ongoing contract management, the financial status of prospective and existing companies is scored for credibility and stability. BC Plans in place by ICT Contractors. 	
CRITICAL BUSINESS AREA					
24/7					
CD 02 Provision of Service Centre	Risk Number as listed in the BIA	Risk Rating taken from the BIA	Risk description as listed in the General BCP	Description of preventative or mitigatory measures. Where these are not in place, they must be addressed in an appropriate action plan.	Description of contingency arrangements. Where these are not in place, they must be addressed in an appropriate action plan.
	CD-02a	16	Loss of Staff		<ul style="list-style-type: none"> Agreed Customer Services Business Continuity plan in place.

OFFICIAL

	CD-02b	8	Loss of Building		<ul style="list-style-type: none"> • Agreed Customer Services Business Continuity plan in place for relocation to Emergency Planning bunker
	CD-02d	16	Loss of ICT	<ul style="list-style-type: none"> • Contractual break/fix arrangements ICT Contract (schedule 8) and PfN contract (part 2.2) for short term losses. • Contractual Disaster Recover/ Business Continuity arrangements - ICT Contract (schedule 9) and PfN contract (part 7.6) for long term losses. • Agreed Business Continuity plans (ELSA) in place with BT for telephony failures. 	<ul style="list-style-type: none"> • Agreed Customer Services Business Continuity plan in place. • Agreed ICT Business Continuity plan in place.
	CD-02f	16	Loss of Utilities	<ul style="list-style-type: none"> • Stand-by generator and UPS facility in the event of loss of power on site. • Regular fuel checks for generator. 	<ul style="list-style-type: none"> • Agreed Customer Services Business Continuity plan in place. • Contact Scottish Water and/or SEPA.
	CD-02h	16	Loss of External Suppliers	<ul style="list-style-type: none"> • As part of Procurement and ongoing contract management, the financial status of prospective and existing companies is scored for credibility and stability. • ICT Contractors BC Plans in place. 	
	CD-02i	20	Excess Demand		<ul style="list-style-type: none"> • Agreed Customer Services Business Continuity plan in place.
	CD-02j	12	Loss of Critical or Sensitive Data	<ul style="list-style-type: none"> • Contractual backup and data restoration arrangements ICT Contract (Schedule 1) and Disaster Recovery arrangements ICT Contract (Schedule 9) • Laptop and USB encryption service enabled to prevent accidental data loss. • Blackberry secure wipe process. • GCSX routing of emailed data between Government agencies. 	<ul style="list-style-type: none"> • Service Description 27 (Backup Service) and Service Description 44 (CRM) detailing back-up and data restoration specific to CRM system.

OFFICIAL

CRITICAL BUSINESS AREA					
24/7					
CD 03 Provision of WAN and LAN	Risk Number as listed in the BIA	Risk Rating taken from the BIA	Risk description as listed in the General BCP	Description of preventative or mitigatory measures. Where these are not in place, they must be addressed in an appropriate action plan.	Description of contingency arrangements. Where these are not in place, they must be addressed in an appropriate action plan.
	CD-03b	16	Loss of Buildings	<ul style="list-style-type: none"> HQ & Nevis House. Capacity to maintain Corporate Internet connection through re-routing if one of them is unavailable. Identify and agree breakout arrangements. Identify, reschedule or relocate critical Council or Hosted meetings. 	<ul style="list-style-type: none"> Rebuild infrastructure in separate location in event of major loss (RFS). Salvage equipment if building is accessible (RFS).
	CD-03d	16	Loss of ICT	<ul style="list-style-type: none"> Contractual break/fix arrangements for the ICT Contract (schedule 8) and PfN contract (part 2.2) for short term losses. Contractual Disaster Recover/ Business Continuity arrangements - ICT Contract (schedule 9) and PfN contract (part 7.6) for long term losses. Contractual escalation for incidents that cannot be managed as part of the standard break/fix process for medium term losses. SSE failover between Mountain and East Coast trunk routes. 	<ul style="list-style-type: none"> Identify and agree breakout arrangements. Agreed ICT Business Continuity plan in place.
	CD-03f	16	Loss of Utilities	<ul style="list-style-type: none"> Reroute of Corporate Internet traffic through Nevis House if experiencing power issues at HQ. 	<ul style="list-style-type: none"> Identify and agree breakout arrangements.
	CD-03h	16	Loss of External Suppliers	<ul style="list-style-type: none"> As part of Procurement and ongoing contract management, the financial status of prospective and existing companies is scored for credibility and stability. BC Plans in place by ICT Contractors. 	

	CD-03l	16	Loss of Compliance and/or Accreditation	<ul style="list-style-type: none"> • Agreed action plans for maintaining PSN accreditation. • Annual ICT Health Checks. • Ad-hoc pen testing • Disclosure checks for relevant staff. 	
CRITICAL BUSINESS AREA					
24/7					
CD 04 Provision of Deaths Registration	Risk Number as listed in the BIA	Risk Rating taken from the BIA	Risk description as listed in the General BCP	Description of preventative or mitigatory measures. Where these are not in place, they must be addressed in an appropriate action plan.	Description of contingency arrangements. Where these are not in place, they must be addressed in an appropriate action plan.
	CA-04a	2	Loss of Staff		<ul style="list-style-type: none"> • Document Business Continuity procedures specific to Service Points. • Agreed National Records Scotland procedures in place.
	CA-04f	4	Loss of Utilities		<ul style="list-style-type: none"> • Document Business Continuity procedures specific to Service Points. • Agreed National Records Scotland procedures in place.
	CD-04i	12	Excess Demand		<ul style="list-style-type: none"> • Document Business Continuity procedures specific to Service Points. • Agreed National Records Scotland procedures in place.
	CD-04j	12	Loss of Critical or Sensitive Data	<ul style="list-style-type: none"> • Contractual arrangements with National Records Office. • Agreed procedures for manually filing data to secure storage. 	
	CD-04l	4	Loss of Compliance and/or Accreditation	<ul style="list-style-type: none"> • Agreed action plans for maintaining PSN accreditation. • Annual ICT Health Checks. • Ad-hoc pen testing • Disclosure checks for relevant staff. • Adherence to proscribed business processes. 	

CRITICAL BUSINESS AREA UP TO 3 DAYS					
CD 05 Provision of CRM System	Risk Number as listed in the BIA	Risk Rating taken from the BIA	Risk description as listed in the General BCP	Description of measures. Where these are not in place, they must be addressed in an appropriate action plan.	Description of arrangements. Where these are not in place, they must be addressed in an appropriate action plan.
	CD-05a	8	Loss of Staff		<ul style="list-style-type: none"> Document Business Continuity procedures specific to Service Points
	CD-05d	8	Loss of ICT	<ul style="list-style-type: none"> Contractual break/fix arrangements ICT Contract (schedule 8) and PfN contract (part 2.2) for short term losses. Contractual Disaster Recover/ Business Continuity arrangements - ICT Contract (schedule 9) and PfN contract (part 7.6) for long term losses. 	<ul style="list-style-type: none"> Document Business Continuity procedures specific to Service Points Agreed ICT Business Continuity plan in place. Agreed manual process in place.
	CD-05f	4	Loss of Utilities	<ul style="list-style-type: none"> Stand-by generator and UPS facility in the event of loss of power at Service Centre. Regular fuel checks for generator. 	<ul style="list-style-type: none"> Document Business Continuity procedures specific to Service Points
	CD-05h	8	Loss of External Suppliers	<ul style="list-style-type: none"> As part of Procurement and ongoing contract management, the financial status of prospective and existing companies is scored for credibility and stability. BC Plans in place by ICT Contractors. 	
CRITICAL BUSINESS AREA UP TO 3 DAYS					
CD 06 Provision of HR Service	Risk Number as listed in the BIA	Risk Rating taken from the BIA	Risk description as listed in the General BCP	Description of measures. Where these are not in place, they must be addressed in an appropriate action plan.	Description of arrangements. Where these are not in place, they must be addressed in an appropriate action plan.
	CD 06a	2	Loss of Staff	<ul style="list-style-type: none"> Identification of critical tasks 	<ul style="list-style-type: none"> Validated call-out details for key staff.

OFFICIAL

				<ul style="list-style-type: none"> • Allocation of critical tasks • Confirmation obtained from third party suppliers and contact details checked • Identify critical areas of ICT access and prepare User Management template for temporary staff. 	<ul style="list-style-type: none"> • Describe the call-out arrangements within the Service BCP. • Ensure contact information for key staff is contained within the Council's Emergency Communications Directory • Identify possible third party advisers from public sector/private sector
	CD 06d	8	Loss of ICT	<ul style="list-style-type: none"> • Identification of any critical ICT in liaison with Digital transformation. • Contractual break/fix arrangements for the ICT Contract (schedule 8) and PfN contract (part 2.2) for short term losses. • Contractual Disaster Recover/ Business Continuity arrangements - ICT Contract (schedule 9) and PfN contract (part 7.6) for long term losses. • Contractual escalation for incidents that cannot be managed as part of the standard break/fix process for medium term losses. 	Agreed ICT Business Continuity plan in place.
	CD 06f	4	Loss of Utilities	<ul style="list-style-type: none"> • Identify and agree breakout arrangements. 	
	CD 06k	12	Loss of Critical or Sensitive Data	<ul style="list-style-type: none"> • Contractual backup and data restoration arrangements ICT Contract (Schedule 1) and Disaster Recovery arrangements ICT Contract (Schedule 9). • Laptop and USB encryption service enabled to prevent accidental data loss. • Blackberry secure wipe process. • Hard copies of critical or sensitive data shall be stored securely in locked cabinets or safes at the end of each working day. • Hard copies of critical or sensitive data not required for archiving, will be shredded immediately. • GCSX routing of emailed data between Government agencies. 	

OFFICIAL

CRITICAL BUSINESS AREA UP TO 3 DAYS					
CD 07 Access to Critical Data	Risk Number as listed in the BIA	Risk Rating taken from the BIA	Risk description as listed in the General BCP	Description of measures. Where these are not in place, they must be addressed in an appropriate action plan.	Description of arrangements. Where these are not in place, they must be addressed in an appropriate action plan.
	CD-07d	16	Loss of ICT	<ul style="list-style-type: none"> Contractual break/fix arrangements ICT Contract (schedule 8) and PfN contract (part 2.2) for short term losses. Contractual Disaster Recover/ Business Continuity arrangements - ICT Contract (schedule 9) and PfN contract (part 7.6) for long term losses. Contractual escalation for incidents that cannot be managed as part of the standard break/fix process for medium term losses. SSE failover between Mountain and East Coast trunk routes. Contractual back-up arrangements for any data stored within the Fujitsu Data Centres. 	<ul style="list-style-type: none"> Identify and agree breakout arrangements. Agreed ICT Business Continuity plan in place.
	CD-07f	16	Loss of Utilities	<ul style="list-style-type: none"> Reroute of Corporate Internet traffic through Nevis House if experiencing power issues at HQ. 	<ul style="list-style-type: none"> Identify and agree breakout arrangements.
	CD-07h	16	Loss of External Suppliers	<ul style="list-style-type: none"> As part of Procurement and ongoing contract management, the financial status of prospective and existing companies is scored for credibility and stability. BC Plans in place by ICT Contractors. 	<ul style="list-style-type: none">
	CD-07j	12	Loss of Critical or Sensitive Data	<ul style="list-style-type: none"> Contractual backup and data restoration arrangements ICT Contract (Schedule 1) and Disaster Recovery arrangements ICT Contract (Schedule 9). 	<ul style="list-style-type: none">

				<ul style="list-style-type: none"> • Laptop and USB encryption service enabled to prevent accidental data loss. • Blackberry secure wipe process. • Hard copies of critical or sensitive data shall be stored securely in locked cabinets or safes at the end of each working day. • Hard copies of critical or sensitive data not required for archiving, will be shredded immediately. • GCSX routing of emailed data between Government agencies. 	
CRITICAL BUSINESS AREA UP TO 3 DAYS					
CD 08 Provision of Legal Service	Risk Number as listed in the BIA	Risk Rating taken from the BIA	Risk description as listed in the General BCP	Description of measures. Where these are not in place, they must be addressed in an appropriate action plan.	Description of arrangements. Where these are not in place, they must be addressed in an appropriate action plan.
	CD 08a	2	Loss of Staff	<ul style="list-style-type: none"> • Identification of critical tasks • Allocation of critical tasks • Confirmation obtained from third party suppliers and contact details checked • Identify critical areas of ICT access and prepare User Management template for temporary staff. 	<ul style="list-style-type: none"> • Validated call-out details for key staff. • Describe the call-out arrangements within the Service BCP. • Ensure contact information for key staff is contained within the Council's Emergency Communications Directory • Identify possible third party advisers from public sector/private sector
	CD 08d	8	Loss of ICT	<ul style="list-style-type: none"> • Identification of any critical ICT in liaison with Digital transformation • Contractual break/fix arrangements for the ICT Contract (schedule 8) and PfN contract (part 2.2) for short term losses. • Contractual Disaster Recover/ Business Continuity arrangements - ICT Contract (schedule 9) and PfN contract (part 7.6) for long term losses. • Contractual escalation for incidents that 	<ul style="list-style-type: none"> • Agreed ICT Business Continuity plan in place.

OFFICIAL

				cannot be managed as part of the standard break/fix process for medium term losses.	
	CD 08f	4	Loss of Utilities	<ul style="list-style-type: none"> • Identify and agree breakout arrangements. 	
	CD 08k	12	Loss of Critical or Sensitive Data	<ul style="list-style-type: none"> • Contractual backup and data restoration arrangements ICT Contract (Schedule 1) and Disaster Recovery arrangements ICT Contract (Schedule 9). • Laptop and USB encryption service enabled to prevent accidental data loss. • Blackberry secure wipe process. • Hard copies of critical or sensitive data shall be stored securely in locked cabinets or safes at the end of each working day. • Hard copies of critical or sensitive data not required for archiving, will be shredded immediately. • GCSX routing of emailed data between Government agencies. 	

OFFICIAL

ACTION PLAN

Outstanding Actions for Corporate Development Business Continuity Plan					
Lead Service:		Corporate Development			
Lead Officer:		Trish Brown	W: 01463 216676	E: trish.brown@highland.gov.uk	
Mitigation		Critical Business Area	Lead Officer	Target date	Date completed
<u>Measure 1</u>	Identification of any critical ICT in liaison with Digital transformation.	CD 06d CD 08d	John Batchelor Stewart Fraser	July 2015	
<u>Measure 2</u>	Enable laptop users for Remote Access if not already enabled.	CD 07d CD 07f	Vicki Nairn	August 2015	
<u>Measure 3</u>	Identify staff for re-location. (laptop users - mobility) (if telephony unaffected, staff may need to remain on site)	CD 03b, d, f CD07d, f CD 06f CD 07d CD 08f	Vicki Nairn Vicki Nairn John Batchelor Stewart Fraser Stewart Fraser	July 2015	
<u>Measure 4</u>	Identify alternative locations for re-deployment of staff (e.g. Archive Centre; Service Centre; Town House, County Buildings; Kinmylies; libraries; Home)	CD 03b, d, f CD 07d, f CD 06f CD 07d CD 08f	Vicki Nairn Vicki Nairn John Batchelor Stewart Fraser Stewart Fraser	July 2015	
<u>Measure 5</u>	To identify and make available necessary equipment to allow additional members of staff to work flexibly in the short term.	CD 06a CD 08a	John Batchelor Stewart Fraser	July 2015	
<u>Measure 6</u>	In case of telephony failure, identify critical telephony numbers for divert and divert location.	CD 03b, d CD 07d	Vicki Nairn	June 2015	

OFFICIAL

<u>Measure 7</u>	Identify, reschedule or relocate critical Council or Hosted meetings	CD 03b CD 07d	Stewart Fraser	August 2015	
<u>Measure 8</u>	Identification and allocation of critical tasks	CD 06a CD 08a	John Batchelor Stewart Fraser	July 2015	
<u>Measure 9</u>	To identify appropriate back up measures or alternatives to ensure critical tasks will continue to be delivered	CD 06a CD 08a	John Batchelor Stewart Fraser	July 2015	
<u>Measure 10</u>	Validate call-out details for key staff	CD 06a CD 08a	John Batchelor Stewart Fraser	June 2015	
<u>Measure 11</u>	Describe call out arrangements	CD 06a CD 08a	John Batchelor Stewart Fraser	June 2015	
<u>Measure 12</u>	Ensure contact information for key staff is contained within the Council's Emergency Communications Directory	CD 06a CD 08a	John Batchelor Stewart Fraser	June 2015	
<u>Measure 13</u>	Identify possible Third Party advisers from the public sector/ private sector	CD 06a CD 08a	John Batchelor Stewart Fraser	July 2015	
<u>Measure 14</u>	Confirmation obtained from third party suppliers and contact details checked	CD 06a CD 08a	John Batchelor Stewart Fraser	July 2015	
<u>Measure 15</u>	Identify critical areas of ICT access and prepare User Management template for temporary staff.	CD 06a CD 08a	John Batchelor Stewart Fraser	July 2015	
<u>Measure 16</u>	Document Business Continuity procedures specific to Service Points	CD 04a, f, i CD 05a, d, f	Tina Page	July 2015	

OFFICIAL

INCIDENT RESPONSE PLAN *(This is to prepare for a timely response to critical incidents and reduce the impact of those incidents on your business operations as identified in your risk assessment. It also prepares key personnel to provide and coordinate an effective response to ensure minimal disruption to business operations in the event of emergency. The following provides an example of the type of information, including checklists, you might include when planning your response to a critical incident. These together would form your Incident Response Plan.)*

Immediate Response Checklist

INCIDENT RESPONSE	✓	ACTIONS TAKEN	REMARKS
Have you:			
• assessed the severity of the incident?	<input type="checkbox"/>		
• evacuated the site if necessary?	<input type="checkbox"/>		
• accounted for everyone?	<input type="checkbox"/>		
• identified any injuries to persons?	<input type="checkbox"/>		
• contacted Emergency Services if necessary?	<input type="checkbox"/>		
• started an Event Log?	<input type="checkbox"/>		
• activated your response plane?	<input type="checkbox"/>		
• activated staff members and resources?	<input type="checkbox"/>		
• appointed a spokesperson?	<input type="checkbox"/>		
• gained more information as a priority?	<input type="checkbox"/>		
• briefed team members on incident?	<input type="checkbox"/>		
• allocated specific roles and responsibilities?	<input type="checkbox"/>		

OFFICIAL

• identified any damage?	<input type="checkbox"/>		
• identified critical business activities that have been disrupted?	<input type="checkbox"/>		
• briefed your Service Director?	<input type="checkbox"/>		
• kept staff informed?	<input type="checkbox"/>		
• contacted key stakeholders?	<input type="checkbox"/>		
• understood and complied with any regulatory/compliance requirements?	<input type="checkbox"/>		
• initiated media/public relations response?	<input type="checkbox"/>		

OFFICIAL

ROLES AND RESPONSIBILITIES *This table allows you to assign responsibility for completion of each task to one of your designated roles. You will then assign each role, or multiple roles, to one or more staff members and assign back-up staff as appropriate. The staff members involved should then be given this table in order to understand their roles and as a task assignment list for completion of pre-emergency planning and emergency tasks.*

Role	Designated Employee(s)	Alternate/Delegated authority
Head of Digital Transformation	Name: Vicki Nairn Contact Information: (01463) 702848	Name: Tina Page Contact Information: (01463) 702707
<p><i>Emergency Responsibilities:</i></p> <ul style="list-style-type: none"> • ensure the Business Continuity Plan for risk CD 01; CD 02; CD 04 or CD 05 has been activated • oversee smooth implementation of the response and recovery section of the plan • determine the need for and activate the use of an alternate operation site and other continuity tasks • communicate with key stakeholders as needed • provide important information to the Communication Officer for distribution • keep key staff apprised of any changes to situation. 		

Role	Designated Employee(s)	Alternate/Delegated authority
Customer Service Manager	Name: Tina Page Contact Information: (01463) 702707	Name: Darren Macleod Contact Information: (01463) 702707
<p><i>Emergency Responsibilities with delegated authority to:</i></p> <ul style="list-style-type: none"> • ensure the Business Continuity Plan for risk CD 01 has been activated • oversee smooth implementation of the response and recovery section of the plan • determine the need for and activate the use of an alternate operation site and other continuity tasks • communicate with key stakeholders as needed • provide important information to the Communication Officer for distribution • keep key staff apprised of any changes to situation. 		

OFFICIAL

Role	Designated Employee(s)	Alternate/Delegated authority	
Customer Service Manager	Name: Tina Page Contact Information: (01463) 702707	Name: Moira Grant Contact Information: (01463) 702707	Name: Ralph Reid Contact Information: (01349) 886776
<p><i>Emergency Responsibilities with delegated authority to:</i></p> <ul style="list-style-type: none"> • ensure the Business Continuity Plan for risk CD 02 has been activated • oversee smooth implementation of the response and recovery section of the plan • determine the need for and activate the use of an alternate operation site and other continuity tasks • communicate with key stakeholders as needed • provide important information to the Communication Officer for distribution • keep key staff apprised of any changes to situation. 			

Role	Designated Employee(s)	Alternate/Delegated authority	
Customer Service Manager	Name: Tina Page Contact Information: (01463) 702707	Name: Moira Grant Contact Information: (01463) 702707	Name: Diane Minty Contact Information: (01463) 256402
<p><i>Emergency Responsibilities with delegated authority to:</i></p> <ul style="list-style-type: none"> • ensure the Business Continuity Plan for risk CD 04 has been activated • oversee smooth implementation of the response and recovery section of the plan • determine the need for and activate the use of an alternate operation site and other continuity tasks • communicate with key stakeholders as needed • provide important information to the Communication Officer for distribution • keep key staff apprised of any changes to situation. 			

Role	Designated Employee(s)	Alternate/Delegated authority	
Customer Service Manager	Name: Tina Page Contact Information: (01463) 702707	Name: Moira Grant Contact Information: (01463) 702707	

OFFICIAL

OFFICIAL

<p><i>Emergency Responsibilities with delegated authority to:</i></p> <ul style="list-style-type: none"> • ensure the Business Continuity Plan for risk CD 05 has been activated • oversee smooth implementation of the response and recovery section of the plan • determine the need for and activate the use of an alternate operation site and other continuity tasks • communicate with key stakeholders as needed • provide important information to the Communication Officer for distribution • keep key staff apprised of any changes to situation.
--

Role	Designated Employee(s)	Alternate/Delegated authority
Head of Digital Transformation	Name: Vicki Nairn Contact Information: (01463) 702848	Name: John Grieve Contact Information: (01463) 702741

<p><i>Emergency Responsibilities:</i></p> <ul style="list-style-type: none"> • ensure the Business Continuity Plan for risk CD 03 or CD 07 has been activated • oversee smooth implementation of the response and recovery section of the plan • determine the need for and activate the use of an alternate operation site and other continuity tasks • communicate with key stakeholders as needed • provide important information to the Communication Officer for distribution • keep key staff apprised of any changes to situation.

Role	Designated Employee(s)	Alternate/Delegated authority
Corporate ICT Manager	Name: John Grieve Contact Information: (01463) 702741	Name: Jon Shepherd Contact Information: (01463) 216636 Name: Linda Johnstone Contact Information: (01463) 216696

<p><i>Emergency Responsibilities with delegated authority to:</i></p> <ul style="list-style-type: none"> • ensure the Business Continuity Plan for risk CD 03 or CD 07 has been activated • oversee smooth implementation of the response and recovery section of the plan • determine the need for and activate the use of an alternate operation site and other continuity tasks • communicate with key stakeholders as needed
--

OFFICIAL

OFFICIAL

- *provide important information to the Communication Officer for distribution*
- *keep key staff apprised of any changes to situation.*

Role	Designated Employee(s)	Alternate/Delegated authority	
Head of Corporate Governance	Name: Stewart Fraser Contact Information: 01463 702112	Name: Julie MacLennan Contact Information: (01463) 702118	Name: Fiona Malcolm Contact Information: (01463) 702114
<p><i>Emergency Responsibilities:</i></p> <ul style="list-style-type: none"> • <i>ensure the Business Continuity Plan for risk CD-08 and CD-07 (for Committee Services) has been activated</i> • <i>oversee smooth implementation of the response and recovery section of the plan</i> • <i>determine the need for and activate the use of an alternate operation site and other continuity tasks</i> • <i>communicate with key stakeholders as needed</i> • <i>provide important information to the Communication Officer for distribution</i> • <i>keep key staff apprised of any changes to situation.</i> 			

Role	Designated Employee(s)	Alternate/Delegated authority	
Head of People & Performance	Name: John Batchelor Contact Information: (01463) 702056	Name: Murdo MacDonald Contact Information: (01463) 702028	Name: Elaine Barrie Contact Information: (01463) 702003
<p><i>Emergency Responsibilities:</i></p> <ul style="list-style-type: none"> • <i>ensure the Business Continuity Plan for risk CD-06 has been activated</i> • <i>oversee smooth implementation of the response and recovery section of the plan</i> • <i>determine the need for and activate the use of an alternate operation site and other continuity tasks</i> • <i>communicate with key stakeholders as needed</i> • <i>provide important information to the Communication Officer for distribution</i> • <i>keep key staff apprised of any changes to situation.</i> 			

OFFICIAL

KEY CONTACT LISTS - Internal

Person	Contact number/s	Email	Responsibilities
Michelle Morris	(01463) 702845 M: 07500101656	Michelle.Morris@highland.gov.uk	<i>All plans</i>
Vicki Nairn	(01463) 702848	Vicki.Nairn@highland.gov.uk	<i>CD 01 CD 02 CD 03 CD 04 CD 05</i>
John Batchelor	(01463) 702056	John.Batchelor@highland.gov.uk	<i>CD 06</i>
Murdo Macdonald	(01463) 702028	Murdo.Macdonald@highland.gov.uk	<i>CD 06</i>
Elaine Barrie	(01463) 702003	Elaine.Barrie@highland.gov.uk	<i>CD 06</i>
Stewart Fraser	(01463) 702112	Stewart.Fraser@highland.gov.uk	<i>CD 08 CD 07d</i>
Julie MacLennan	(01463) 702118	Julie.Maclennan@highland.gov.uk	<i>CD08 CD07d</i>
Fiona Malcolm	(01463) 702114	Fiona.Malcolm@highland.gov.uk	<i>CD08 CD07d</i>
Tina Page	(01463) 702707 M: 07748 148035	Tina.Page@highland.gov.uk	<i>CD 01 CD 02 CD 04 CD 05</i>
Darren MacLeod	(01463) 702707 M: 07818 520122	Darren.Macleod@highland.gov.uk	<i>CD 01</i>
Ralph Reid	(01349) 886776 M: 07716 623666	Ralph.Reid@highland.gov.uk	<i>CD 02</i>
Diane Minty	(01463) 256402 M: 07818 588203	Diane.Minty@highland.gov.uk	<i>CD 05</i>
Moira Grant	(01463) 702707	Moira.Grant@highland.gov.uk	<i>CD 04</i>
John Grieve	(01463) 702741 M: 07557 480844	John.Grieve@highland.gov.uk	<i>CD 03 CD 07</i>

OFFICIAL

Jon Shepherd	(01463) 216636 M: 07733 301919	Jon.Shepherd@highland.gov.uk	<i>CD 03</i> <i>CD 07</i>
Linda Johnstone	(01463) 216696 M: 07786 171705	Linda.Johnstone@highland.gov.uk	<i>CD 03</i> <i>CD 07</i>

OFFICIAL

KEY CONTACT LISTS - External

Key Suppliers	Contact	Contact number/s															
Suppliers	<p>Fujitsu Services: Catriona MacDonald, Account Director</p> <p>Also for third parties: KANA (CRM); Netcall (Service Centre); Jadu (Website) Northgate Arinso (HR/Payroll)</p>	Mobile: (07867) 822314															
	<p>Vodafone (Pathfinder): Martin Thomson, Service Manager</p> <p>Vodafone (Mobile telephony): Norman Yuill, Corporate Account Development Manager - Public Sector</p>	<p>Mobile: 07909 978554</p> <p>Mobile: 07836 241118</p>															
	<p>Capita:</p> <table border="1" data-bbox="465 1066 1700 1347"> <thead> <tr> <th>Contact</th> <th>Contact Number</th> <th>Service Hours</th> <th>Contact Email</th> </tr> </thead> <tbody> <tr> <td>Service Desk</td> <td>0808 169 2555</td> <td>24x7</td> <td>SWANServiceDesk@capita.co.uk</td> </tr> <tr> <td>Change Management</td> <td>0808 169 2555</td> <td>24x7</td> <td>SWANChangeMgmt@Capita.co.uk</td> </tr> <tr> <td>Major Incident Management</td> <td>0808 169 2555</td> <td>24x7</td> <td>SWANMajorIncident@Capita.co.uk</td> </tr> </tbody> </table>		Contact	Contact Number	Service Hours	Contact Email	Service Desk	0808 169 2555	24x7	SWANServiceDesk@capita.co.uk	Change Management	0808 169 2555	24x7	SWANChangeMgmt@Capita.co.uk	Major Incident Management	0808 169 2555	24x7
Contact	Contact Number	Service Hours	Contact Email														
Service Desk	0808 169 2555	24x7	SWANServiceDesk@capita.co.uk														
Change Management	0808 169 2555	24x7	SWANChangeMgmt@Capita.co.uk														
Major Incident Management	0808 169 2555	24x7	SWANMajorIncident@Capita.co.uk														

OFFICIAL

	British Telecom: Alex Swart, Account Manager	Tel. (01977) 592376 Mobile 07850 753037
	Jadu Universe CMS Telephone +44 (0)116 222 7242 Email info@jadu.net Jadu Global Head Quarters, Universe House, 1 Merus Court, Leicester, LE19 1RJ United Kingdom	
	Registers of Scotland Meadowbank House, 153 London Road Telephone 0800 169 9391	
Facilities Management HQ	Yvonne Henderson Barry Kane	Tel. (01463) 216638 Tel. (01463) 702280

OFFICIAL