Skills 4 Stem Ltd.
Tackling the STEM skills shortage

Business/Delivery Continuity Plan

Version	Author	Description
V1	Rob Davis	Issue Jan 2018
V2	Sarah Davis	Issue Jan 2019
V3	Sarah Davis	Issue June 2019

Contents

Document description 3

Actions to be taken 3

Risks 4

Planned Incident Responses (PIR) 5

Who 7

Procedures arising from PIRs 9

Business Continuity Plan Lifecycle BCPL 9

Document description

This document identifies risks and designates the processes and expected actions when a Business Continuity Plan incident takes place.
The Business Continuity Plan (BCP) is continually evolving and the BCP lifecycle is defined in the last section. This is to ensure that apprentice/candidate delivery is not disrupted should incidents or accidents occur including flood, fire, terrorism activity etc.

Should action be taken?

Risks to organisation and apprenticeship/candidate delivery

Risks, as defined here are “high level” and common sense should be used when an incident not explicitly described is encountered.

Risk	Impact	Response
Communication systems breakdown	No access to candidates/apprentices/staff /employers	We use a web based telephony system to ensure contact is available from anywhere in the world. However, should this breakdown we will use other methods including mobile telephones and office telephones. We have email addresses for all candidates/apprentices.
Transport issues	Staff, volunteers, apprentices/candidates cannot access the office or training facility	Should transport issues affect attendance then delivery can take place at a different venue, a different date or via web links. We have access to various venues and can move delivery immediately and our ICT systems are web based therefore candidate/apprentice delivery will not be disrupted.
No access to main office building	No access to IT or telephony equipment. Including onsite-training facilities.	Escalation and dissemination of status. (see PIR below) Skills4Stem operational staff will be asked to work from home until an alternative office is available utilising web-based communication and telephony services and live web chat.
No access to specific designated training/site location	No training/assessing can take place.	Escalation and dissemination of status. (see PIR below) Skills4Stem will make arrangements for all candidates to be trained at an alternative location. We have access to Regis offices therefore a resolution to this is available immediately.
Equipment damage/loss (computers)	Impact limited to uniqueness of information stored on equipment.	Escalation. Seek specific PIRs related to data security/recovery.

Equipment damage/loss (other)	Cannot use/operate that specific piece or pieces of equipment.	Escalation. Seek specific PIRs related to equipment nature.
3rd party service failure	Access and processing of records maybe delayed.	Escalation and dissemination of status. (see PIR below)
Communications systems failure	Access and processing of records maybe delayed.	Escalation and dissemination of status. (see PIR below)
Health and Safety or Prevent/Bullying/Harassment incident	Priority shift to resolve incident.	Record incident and escalate. (see PIR below). Skills4Stem to contact supervisory 3rd parties as required.
Fire, Flood, Terrorism	Staff, volunteers, apprentices/candidates cannot access the office or training facility	Should these issues affect attendance then delivery can take place at a different venue, a different date or via web links. We have access to various venues and can move delivery immediately and our ICT systems are web based therefore candidate/apprentice delivery will not be disrupted.
Data loss/breach, virus/malware/ransomware.	Reduced access to systems and data.	Escalation. Seek specific PIRs related to data security/recovery. Report to 3rd parties involved as required.
Lack of access to specific personnel. Internal or external	Reduced access to business processes.	Escalation. Review specific PIR
Loss of key personnel	Leadership and management of the business	The SMT includes members of the board, therefore all are familiar with business critical strategies. All occupational sectors have more than 1 qualified and experienced deliverer therefore training need not be disrupted.

Planned Incident Responses (PIR)

PIRs, as defined here are “high level” and common sense should be used when an incident not explicitly described is encountered.

PIR Type	Actions
Access to main building	When there is a total loss of access to the main building due to flood/fire etc. The CEO must be informed. The CEO or equivalent will then disseminate the status to the relevant parties, internal and external (see **Who** below). They will also monitor the situation and advise when the “all clear”/” stand down” is given.
Access to training or site location	The CEO must be informed. The CEO or equivalent will then disseminate the status to the relevant parties, internal and external (see **Who** below). They will also monitor the situation and advise when the “all clear”/” stand down” is given.
Computer equipment damage	The CTO should be informed. They will then review cause, resolution and future mitigation. Replacements will be provided, as required, where possible, immediately. Concerns around data loss and recovery will also be investigated on a case by case basis.
Computer equipment loss	The CTO should be informed. All lost equipment is to be considered “compromised” and immediate action taken to secure any and all systems from adversarial action. Included actions should include reviewing possible data loss, data theft and change of passwords/access.
3rd party failure	CEO/CTO should be informed. Skills4Stem currently relies on the following main 3rd parties Infusionsoft; CRM. When CRM data is unavailable all sales activity will stop until resolved. Accepted risk. 1and1; Moodle, website and DNS. No online presence will be available, and candidates will be unable to access the LMS. Data is backed up and based on “down time” a new website provider may need to be employed. G-Suite; Google drive and email No email communication and no access to online documentation. All important documents will be available offline. Accepted risk.
Loss of telephony services	The CEO must be informed. They will advise FM/telephony provider (Moneypenny). Status will be disseminated to relevant parties.
Loss of email	The CTO should be informed. Email and paper will be used in the short term. They will advise email provider. Status will be disseminated to relevant parties.

Loss of internet	The CTO should be informed. They will advise FM/telephony provider (Moneypenny). Status will be disseminated to relevant parties.
Data security	The CTO should be informed. Data security policy to be followed. Including possible data recovery.
Data loss	The CTO should be informed. Data security policy to be followed. Including possible data recovery.
Health and Safety or Prevent/Bullying/Harassment incident	The CEO must be informed. They will then follow the relevant Safeguarding, Prevent and Health and Safety policies and procedures.
Power loss	The CEO must be informed. They will advise FM. Status will be disseminated to relevant parties. The CEO or CTO will decide if the danger requires office evacuation.
Heating loss	The CEO must be informed. They will advise FM. Status will be disseminated to relevant parties. The CEO or CTO will decide if the danger requires office evacuation.
Facility loss, toilets clean water etc	The CEO must be informed. They will advise FM. Status will be disseminated to relevant parties. The CEO or CTO will decide if the danger requires office evacuation.
Company credit card	Access to the company credit card is currently maintained by the CEO only. Accepted risk.
Document access	Access to documentation required for the business to function is held off site and is accessible be the CEO and CTO. Including Insurance documentation Client information Contracts Supplier details
Personnel	See the “Who” list below for details for contact details and escalations.
Legal	The CEO must be informed. They will then seek legal counsel.

Who

Title	Name/s	Contact details	Superior
CEO	Sarah Davis	07967 942962 sarah@skills4stem.co.uk	None, please contact Rob Davis CTO
CTO	Rob Davis	07793 885086 rob@skills4stem.co.uk	Sarah Davis CEO
Operations Manager	Tracy Butler	07598 336226 tracy@skills4stem.co.uk	Sarah Davis CEO / Rob Davis CTO
Customer Services	Sonia Kaur Masciopinto	07403 282821 sonia@skills4stem.co.uk	Tracy Butler (Ops Manager)
Sales team	Joanna Daly Mishall Manji	joanna@skills4stem.co.uk 07747 052601 mishall@skills4stem.co.uk	Sales Manager / Tracy Butler (Ops Manager)
Assessors	See Assessor Details file	Master Apprenticeship Candidate Sheet & Assessor Details file	S4S Head of Quality / Tracy Butler (Ops Manager)
Trainers	See Trainer Details file	Master Apprenticeship Candidate Sheet & Trainer Details file	S4S Head of Quality / Tracy Butler (Ops Manager)
Apprentices	Master Apprenticeship Candidate Sheet	Master Apprenticeship Candidate Sheet	Apprentice line manager / HR / S4S Quality Manager
Apprentice line manager	Master Apprenticeship Candidate Sheet	Master Apprenticeship Candidate Sheet	HR/ 3rd party contact/ S4S Head of Quality
HR/ 3rd party contact	n/a	Master Apprenticeship Candidate Sheet	S4S Head of Quality / Sarah Davis CEO
FM support (main office)	Simon Dunning	Bedford I-lab Stannard Way, Bedford MK44 3RZ 01234 834564	Sarah Davis CEO / Rob Davis CTO
Legal	Edward Lee	Howes Percival LLP Bell House, First Floor Seebeck Place, Knowlhill Central Milton Keynes Buckinghamshire	Sarah Davis CEO / Rob Davis CTO / Tracy Butler (Ops Manager)

		MK5 8FR 01908 672682	
Education and Skills Funding Agency (ESFA)	Denise Young (ESFA Territory Manager)	Cheylesmore House 5 Quinton Road Coventry CV1 2WT Tel: 0370 000 2288	
Accountants	Ross Lane	Mercer & Hole Milton Keynes Silbury Court 420 Silbury Boulevard Central Milton Keynes MK9 2AF Tel: +44 (0)1908 605552 miltonkeynes@mercerhole.co.uk	Sarah Davis CEO / Rob Davis CTO
Health and Safety Executive	hse.gov.uk	Woodlands Manton Lane Manton Lane Industrial Estate Bedford MK41 7LW	

Procedures arising from PIRs

Escalation: The "**Who**" list above defines where escalations should go.
Reporting: Escalation channels will ensure all necessary documentation is completed.
Alerts/Alerting: Escalation channels will ensure all required messaging is disseminated to the necessary parties.

"All clear"/"Stand down": Escalation channels will ensure all required parties are notified of the status change.

Out of Hours: Contact CEO/CTO

Business Continuity Plan Lifecycle BCPL

The BCPL includes regular reviews and updates. When significant changes are noticed and relevant, they are to be disseminated to the relevant personnel and may entail additional training/documentation.

When a PIR is completed and the “all clear” is given, it is strongly recommended that a retrospective is taken to review future prevention and mitigation.

To test the validity of the BCP the following will be enacted on a regular basis.

- Paper exercises; Commonly used during the review process to identify impact and responses.
- Drill basic; Enact a simple PIR, with a small number of staff
- Drill full; Enact a complex and possibly multiple PIRs of most staff