



Name; TSC 053  
 Document Version: V2  
 Originally drafted: 23<sup>rd</sup> February 2019  
 Last Reviewed: 21<sup>st</sup> December 2021  
 Next Review Date: 21<sup>st</sup> December 2022  
 Author: Support Services

**THE SKILLS CENTRE - BUSINESS CONTINUITY PLAN**

<b>Impact</b>	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		<b>Likelihood</b>		

	<b>Vulnerability / Threat</b>	<b>Likelihood (High, Medium, Low)</b>	<b>Impact / Consequence (High, Medium, Low)</b>	<b>Risk Level (High, Medium, Low)</b>
<b>1</b>	Server Failure	L	M	M
<b>2</b>	Fire	L	H	M
<b>3</b>	Flooding	L	M	L
<b>4</b>	Disruption to Transport links	M	L	L
<b>5</b>	Criminal – Theft, Break-ins and Vandalism	L	M	L
<b>6</b>	Sabotage	L	H	M
<b>7</b>	IT – Viruses, Hacking and Unauthorised Intrusions.	L	H	M
<b>8</b>	IT – Communications and Connectivity	L	L	L
<b>9</b>	Aggressive Competitor	M	M	M
<b>10</b>	Finance	L	H	H



11	Pandemic - Specific measures related to Covid 19	L (H)	H	H
----	---	----------	---	---



<b>10</b>	Emergency Contacts	N/A
-----------	--------------------	-----

**This Operation is to be undertaken by a fully trained or supervised by a fully trained/authorised person**

	Vulnerability / Threat	Impact / Consequences	Prevention Strategy	Response / Recovery Strategy	By whom and by when
<b>1</b>	Server Failure	<p>Loss of historical information.</p> <p>Disruption to business operations that require server use.</p>	Server is backed up daily remotely by external appointed IT contractor.	<p>Inform appointed contractor of the issue and take remedial action to resolve the issue.</p> <p>Existing server backed up by contractor or new server purchased and backed up data installed.</p>	<p>Management to report to contractor immediately</p> <p>External Contactor to resolve the problem asap.</p>
<b>2</b>	Fire	<p>Building Damage, resulting in disruption to daily business operations.</p> <p>Loss of information and technology.</p>	<p>Fire Risk Assessment completed for each premises and proactive fire prevention, precautions and procedures adapted.</p> <p>Building and contents insurance acquired.</p>	<p>Short term rental of new premises to minimise business disruptions.</p> <p>Insurance claim to be filed.</p> <p>Replacement I.T equipment to purchased and backed up by remote server to enable day to day business operations.</p>	<p>Directors – asap.</p> <p>Directors – asap</p> <p>Directors - asap</p>



			Remote server for historical record keeping.	Learners and clients informed of change in location/circumstances to ensure no interruption to learning	Admin - asap
<b>3</b>	Flooding	Building Damage, resulting in disruption to daily business operations.  Loss of information and technology.	Building is located in a low risk area for flooding.  Building and contents insurance acquired.  Remote server for historical record keeping.	Short term rental of new premises if required to minimise business disruptions.  Insurance claim to be filed.  Learners and clients informed of change in location/circumstances to ensure no interruption to learning	Directors – asap  Directors – asap  Admin - asap
<b>4</b>	Disruption to Transport links	Major transport disruption  Disruption/Delay to business operations and teaching and learning.	Consideration of transport requirements and accessibility for identified premises.  Wide ranging routes and modes of transport identified and shared with staff and learners	Transport disruption communicated to learners and staff via text/email.  Alternative routes and modes advised  If necessary self-directed study tasks to be activated against ILPs via e-portfolio system to ensure no interruption to learning	Lead Instructor – asap  Instructor Team - asap  Operations Director – asap



5	Criminal – Theft, Break-ins and Vandalism	<p>Building Damage, resulting in disruption to daily business operations.</p> <p>Loss of information and technology.</p> <p>Loss of staffing power.</p>	<p>Good Building security features installed, such as alarm system and roller shutters.</p> <p>Locked access to information throughout the building via internal keypad doors.</p> <p>Building and contents insurance acquired.</p>	<p>All staff personnel to report on any information or technology losses during a theft or break-in.</p> <p>Police to be informed and Insurance claim to be filed.</p> <p>Technology equipment to purchased and backed up by remote server to enable day to day business operations.</p> <p>Third parties informed of any relevant information that may have been stolen that could have adverse effects.</p>	<p>Staff -asap</p> <p>Directors - asap</p> <p>Directors –asap</p> <p>Management team lead by Directors - asap</p>
6	Sabotage	<p>Loss, theft or destruction of sensitive information.</p> <p>Potential Data Protection Breach</p>	<p>Controlled Access to sensitive information.</p> <p>Disclosing information clause encompassed in to employment contracts.</p>	<p>Once sabotage has been detected within the company a thorough investigation to minimise adverse business effects. Determine who is responsible and appropriate legal action to be taken if required to safeguard stakeholders and financial interests.</p>	<p>Directors – asap</p>



		Loss of contracts and/or business to competitors affecting the company's finances.		Compliance of GDPR - Data Protections Rules and Regulations	
<b>7</b>	IT – Viruses, Hacking and Unauthorised Intrusions.	<p>Loss, theft or destruction of sensitive information.</p> <p>Corruption of hardware and software, leading to loss of productivity.</p> <p>Bribery from information obtained by unauthorised access.</p>	IT consultant acting on behalf of the company to identify any potential threats and act accordingly to prevent adverse effects.	<p>Staff to inform admin team of any IT issues that may have adverse effects.</p> <p>Admin team to liaise with the IT consultancy of any reported issues and remedial action to be taken.</p> <p>Staff informed of any remedial action they must complete by the admin team to reduce current/future risks to IT equipment.</p>	<p>All staff- asap</p> <p>Staff Team –within 1 hour of original report</p> <p>Staff team – within 24 hours of reported issues</p>
<b>8</b>	IT – Communications and Connectivity	Disruption to business operations that require external communications and connectivity with learners, clients and staff.	<p>IT consultant acting on behalf of the company to rectify any communication or connectivity issues.</p> <p>Scheduled maintenance is</p>	<p>Staff to be informed of any communications and/or connectivity issue by admin team or vice versa.</p> <p>Admin team to liaise with the IT consultancy and/or service provider of any reported issues and sort</p>	<p>Staff team – asap</p> <p>Staff Team –within 2 hours of original report</p>



			<p>conducted out of normal operational hours when practicable.</p> <p>4g enabled devices issued to staff so remote working can take place when Wi-Fi connectivity is down and/or not available.</p>	<p>advice and update on remedial action to be taken.</p> <p>Remote working to take place as far as practical until communication or connectivity issue have been fixed.</p> <p>Any frequent reports of connectivity or communication reports to be investigated and a change of service provider may be appointed by the company.</p>	<p>All staff – on-going</p> <p>Director responsible for Health &amp; Safety – to raise at next board meeting</p>
9	Aggressive Competitor	<p>Loss of contracts and/or business to competitors affecting the company's finances.</p> <p>Loss of staff to competitors.</p>	<p>Adopt a strategical marketing strategy benchmarked against similar companies to remain competitive within the sector.</p> <p>Provide an attractive employment contract and value staff to maintain a good staff retention rate.</p>	<p>Business development team to assess the competitors services and were practical and sustainable adapt our own marketing strategy to compete with any aggressive competitors.</p>	<p>Business Development Team – as instructed by the Directors</p>







		relation to Covid 19.  Testing and mitigation for Covid (Omicron Variant)	reviewed in line with Government guidance to ensure we are compliant within the regulations. Updated as from the 4 <sup>th</sup> January 2022	Lateral Flow tests are carried out prior to students entering classrooms with the addition of masks now being worn again in classrooms	
--	--	---	---	--	--



<b>12</b>	Emergency Contact Details	JOHN WHITE Ops Director  ESFA	Phone Number  02036211937  0370 000 2288	e-mail  john.white@theskillscentre.co.uk  Department of Education  Gov.uk	