Chelsea Theatre Business Continuity Plan for Data and Cyber Security

Last Date of review	Document signed off by	Document distributed to (e.g. registered manager, management team, directors, trustees)
22/02/2024	Paul Adlam	Management Team

Digital systems	Rate the impact of these systems failing in terms of severity (1 – 10) 1 being low, 10 being high	Can you use an alternative method e.g. paper – based alternative? If so where is this stored?	Date Completed
Email (Outlook)	10	No alternative	22/02/2024
Drop box	2	No Alternative	22/03/2024
Xero	10	No Alternative	22/02/2024
One Drive	6	No Alternative	22/02/2024
Share point	4	No Alternative	22/02/2024
Spektrix	4	No Alternative	22/02/2024

Device	Rate the impact of these systems becoming broken/lost/stolen in terms of severity (1 – 10) 1 being low, 10 being high	Date Completed
Lap tops x 3	1	22/02/2024
Desktop computers x 5	1	22/02/2024
Work phones x 4	1	22/02/2024

1.1 Critical systems and devices

Complete one row below for any system or device rated over a 5 in severity (in 3.1 and 3.2 above) – these are our 'critical systems'.

Critical systems	Provider / Contact details	For critical systems: Does the supplier have their own business continuity plan in place? Where can this be found?	Date Completed
Email	Outlook	https://learn.microsoft.com/en-us/compliance/assurance/assurance-resiliency-and-continuity	22/2/2024
Accounting	Xero		
File storage	One drive	https://learn.microsoft.com/en-us/compliance/assurance/assurance-resiliency-and-continuity	22/2/2024

2. Business continuity: scenarios

Consider	Continuity plan
How will we access our systems and data e.g. • **what other computers can we use** • **where will we work from** • **can we get our data back from our backups** • **how will we access the internet (e.g. for email and other online systems)**	All cloud based systems are accessible remotely. They will be accessed from hired or new machines off site.
If this happens, who needs to do what, and by when	CEO and OM to organise key staff access to new hardware.
Who needs to be told and how will we tell them	All staff
What needs to be put in place so that our plan will work, who will do this and by when	Source suppliers. Can be actioned if needed.

Consider	Continuity plan
What external telephone numbers are critical to running the business and how will we know what numbers these are?	Stored on shared drive
What will we use to make phone calls?	Work or personal mobile phones
How will we connect to the internet (e.g. for email, and any other online critical systems)	by using a 'dongle' or mobile phone wifi hotspot or home broadband
If this happens, who needs to do what, and by when	No Action needed until necessary
Who needs to be told and how will we tell them	All staff
What needs to be put in place so that our plan will work, who will do this and by when	No action needed until necessary. CEO and OM responsible.

What would happen in the event of a power outage?

Consider	Continuity plan
How will we access our systems and data e.g. • **where will we work from** • **what computers can we use** • **how will we access the internet (e.g. for email and other online systems)** • **For critical systems that are not online, how can we access what we need?**	During an extended power outage in the building staff would work from home or other remote venue. All information cloud based. No Critical systems not online. All visitors due to the building to be notified by phone or email. Closure signage in place on building.
If this happens, who needs to do what, and by when	Action immediately by FOH and Management
Who needs to be told and how will we tell them	colleagues, other organisations, relevant stakeholders dependent on length of outage
What needs to be put in place so that our plan will work, who will do this and by when	No Action necessary to prepare.

2.1 Scenario 4 - What would happen if a device failed? What would happen if a device became lost or stolen?

Consider	Continuity plan
How will we access our systems and data e.g. • **what other device/s can we use** • **if necessary, can we get our data back from our backups** • **how will we prevent our data getting into the wrong hands**	All cloud systems accessible from other devices. All devices required to have two factor identification.
If this happens, who needs to do what, and by when	Loss to be reported by staff member to CEO or OM immediately.
Who needs to be told and how will we tell them	N/A

What needs to be put in place so that our plan will work, who will do this and by when	set up a spare computer ready to use make sure information can be restored from our (regular) backups make sure our devices are difficult to get into, by using encryption or two factor authentication; using strong passwords / pins; fingerprint or facial recognition e.g. make sure that lost or stolen devices can be tracked and 'wiped' remotely Bring your own device Bring Your Own Device policy to cover arrangements for personal devices (e.g. such as a smartphone)

2.2 Scenario 5 - What would you do if you were hacked?

Consider	Continuity plan
If this happens, who needs to do what, and by when	**Contact Action Fraud** Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cyber crime. You can report fraud or cyber crime using their online reporting service any time of the day or night; the service enables you to both report a fraud and find help and support. You can talk to their fraud and cybercrime specialists by calling 0300 123 2040 **Follow the breach reporting procedure** For a data security breach incident reporting form see: https://www.digitalsocialcare.co.uk/resource/data-security-breach-incident-reporting-form-template/ **Change passwords** Passwords should only ever be changed if they've been compromised, this is an instance where they would need to be changed **Obtain technical advice and support** IT Support can help with repairing computers if this is needed **Restore backups** If necessary, as a way of retrieving your information

Who needs to be told and how will we tell them	All staff, Relevant trustees
What needs to be put in place so that our plan will work, who will do this and by when	
What prevention measures do we have in place in terms of our technical approaches?	Keep operating systems and software up to date for all devices Use anti-virus software on computers and laptops Implement a firewall for your offices' internet connections Avoid unsecure or public Wi-Fi
What prevention measures do we have in place in terms of staff training?	Staff awareness training – as part of induction Reminders and/or retraining annually

2.3 Scenario 6 - What would happen if a supplier had a fault? i.e. the care planning system won't work and it's the supplier's fault?

Xero, Dropbox or Microsoft fail sufficiently rarely that continuity plans are not typically necessary.

Consider	Continuity plan
What critical aspects of our business will be affected?	All
How will we access the information that we need?	Suspending business until issue resolved. Putting a temporary spreadsheet system in place
If this happens, who needs to do what, and by when	CEO or OM FM or PM to contact relevant supplier.
Who needs to be told and how will we tell them	All Staff & relevant trustees
What needs to be put in place so that our plan will work, who will do this and by when	local daily backups which could then be restored weekly paper printout of the rota OM