IT and Estates Risk Control Register

Risk Category	Activity	Top Risk(s)	Initial Likelihood	Initial Severity	Initial Risk Rating	Prevention Controls - reducing likelihood	Mitigation Controls - reducing severity	Final Likelihood	Final Severity	Final Risk Rating	Responsibility?	Last / next review
	IT Systems											
1	Cyber attack	• Virus, ransom-ware or other malware attack or software vulnerability. • Malicious software can damage IT system, steal or encrypt data or prevent normal service by sheer volume of extra traffic. • Problem could spread to many servers, computers and/or other devices and take days/weeks to clear. • Denial of Service Attacks could affect internal or external systems. • Reputational damage can result from cyber attack.	4	5	20	• Anti-virus & anti-malware software is used on all servers & computers. These are updated automatically in real-time. • Software updates & security patches are applied automatically from O365 tenant ring group. • Firewalls control unauthorised entry from Internet. Web filtering software prevents users from accessing unsafe websites. Email filtering blocks most unsafe emails. • Staff are educated to avoid risks from phishing attacks. Simulated attacks are used to ensure that staff comply. Mandatory training now includes cyber security for all staff. • Enforced use of strong passwords and MFA.	• Multiple backups of data are maintained on a daily/monthly basis. • Wasabi & HYCU cloud backup solution of data are maintained on a daily/monthly basis. • Backups are both on-line and off-line to maximise opportunity for data recovery. • Data has now been migrated to Microsoft and other hosted platforms. • Cyber Insurance acquired to provide cover for additional work in recovery and restoration	3	4	12	Dir of IT & Est	Jan 24 / Apr 24
2	IT System - LAN / WAN Failure	• Switch / Router failure or configuration corruption / deletion • Firewall failure or configuration corruption / deletion	3	5	15	• Firmware and software updated regularly. • Use of strong passwords. • Access limited to essential personnel.	• Spanning tree protects against single device failure by rerouting connections. • High availability firewalls allow one firewall to take over if another fails. • Cloud firewalls are updated automatically and can failover to a second Zen internet connection if needed. • Spare switch ready configured for replacement • Backup copies of all configs kept securely	2	4	8	Dir of IT & Est	Jan 24 / Apr 24
3	IT System - Server / SAN Failure	• Major hardware failure can be caused by a range of events, both accidental and malicious. Depending on which hardware fails, vital services could be disrupted or communications lost.	3	5	15	• For Servers and NAS, dual components provide redundancy for single item failures. • Global spare disks enable automatic replacement of a failed drive. • Firmware and software updated regularly. • Use of strong passwords. • Access limited to essential personnel.	• Warranty support contracts provide rapid response to replace failed parts. • Regular backups of virtual servers enable rapid recovery in event of failure. • Servers and disks now managed by third party and updates handled by them.	2	4	8	Dir of IT & Est	Jan 24 / Apr 24
4	Loss of Key Personnel	• Some systems may be understood by only one person, who could leave, become ill, have an accident, etc. Some systems could then be difficult to maintain, with extended downtime, or projects could be delayed.	3	5	15	• Recruiting to a higher level second role to help spread the critical systems knowledge	• The IT Department has a Network Administration Guide (NAG) which details all aspects of the configuration of the IT system & also details the support tasks which must be performed by new or contract staff. • Training to other IT personnel is ongoing to upskill them. • Some aspects of the IT system now covered by a co managed SLA with a third party IT contractors.	2	4	8	Dir of IT & Est	Jan 24 / Apr 24
5	Theft of data	• Theft of data would compromise privacy laws (GDPR) & could affect reputation.	3	4	12	• All system data is protected by strong IT system access security (usernames & passwords) & where needed MFA. Data is only made available to staff on a need-to-know basis. • Data access is regularly reviewed. • Data cannot be taken offsite as all writable media (CD/DVD, USB, etc) are disabled except for IT issued encrypted USB pens. Web filtering prevents access to file transfer services. • Unauthorised access is prevented by using MAC address authentication on all switch ports & VLANs to segregate data areas. • Office 365 emails & other services are encrypted & monitored to prevent unauthorised data transfer.		1	4	4	Dir of IT & Est	Jan 24 / Apr 24
6	Failure of Outsourced Services	• Potential for loss of service from outsourced services (including Mircosoft Azure, O365, EMIS, anti-virus, remote access, HR, Sage Cloud). • Service quality and security possibly at risk. • Reputation possibly at risk.	2	5	10	• Contractual agreements with third party suppliers. • Service providers have multiple data centres in different locations for data resilience. • Service providers perform regular backups and regular security updates. • Service providers use strong passwords and some use 2FA.	• Emails are available on mobile devices for some staff. • Hybrid environment allows access to login in onsite to enable access to clinical system if available. • Daily paper print-outs are used to enable continued operation in the event of an EMIS failure.	2	4	8	Dir of IT & Est	Jan 24 / Apr 24
7	Mains power failure to vital IT equipment.	• Powerdown of key equipment would disable electronic communication and central IT services.	2	5	10		• Key equipment supported by UPS batteries. Standby generator starts within minutes. • Generator tested regularly. UPS batteries replaced when needed.	2	3	6	Dir of IT & Est	Jan 24 / Apr 24
8	Loss of or corrupted backups	• Backups of data are essential to protect against loss or damage to live production data storage	2	5	10	• Backups are stored securely in main Server Room & locked IT Store Room, with strictly controlled access. • One backup copy is held off-line to protect against cyber attack.	• Data is protected by multiple levels of backup copies. • Data is backed up weekly, daily or more frequently, as required. • Data retention policy is 3 months in accordance with GDPR. • Backups are also stored in cloud with Wasabi and Datto.	2	3	6	Dir of IT & Est	Jan 24 / Apr 24
9	• Loss of Internet (leased line) connection • Loss of EES (Capitol House) connection • Loss of NHS HSCN connectoin	• Loss of any of the 3 connection services is likely to be due to third party problems and therefore outside our control. • Loss of the Internet connection would affect access to all web based information and email services. Software services which are hosted on-line would not be accessible. • Loss of the NHS HSCN line would prevent access to the EMIS PID system. • Loss of access to the EES line would prevent Capitol House staff from accessing the main network.	2	5	10		• SLAs with the line providers guarantees fastest possible recovery from loss of service. • Emails are available on mobile devices for some staff. • Hybrid environment allows access to login in onsite to enable access to clinical system if available. • EMIS users could access EMIS mobile from an alternative internet connection using their login. • Capitol House staff could use computers based in the main site or remotely until the problem is resolved. New Firewall high availability allows the automatic switch over to a second firewall socket or to a second broadband connection (Zen).	2	4	8	Dir of IT & Est	Jan 24 / Apr 24

10	Loss of telephone connection	• Loss of VoIP telephone connection would disrupt all normal voice communication, and could be a major problem in an emergency such as a fire.	3	3	9		• Alternative arrangements are already in place to protect against a VoIP system failure & these have been tried & tested. • Two emergency mobile phones are available for incoming & outgoing calls respectively. • Incoming direct-dial numbers can be re-directed during a fault to the incoming mobile phone. These mobiles (& staff mobiles) can be used for fire, ambulance & police emergency calls if required.	3	2	6	Dir of IT & Est	Jan 24 / Apr 24
	ESTATES											Jan 24 / Apr 24
1	Loss of Electrical Power	• Loss of mains power to part or the whole of the Hospice site could cause major disruption for staff & patients.	2	5	10		• In the event of a mains power failure, the Hospice diesel generator will start automatically & "cut-in" within minutes. • During this time, however, all equipment (unless battery powered) will shutdown & need to be rebooted when power returns. • All parts of the Hospice Main Building are supported by the emergency generator, but not 759 building or St. Bedes.	2	3	6	Dir of IT & Est	Jan 24 / Apr 24
2	Fire	• A fire can occur in any location, being caused by various events. Fires can have a major effect on the use of the location involved.	2	5	10	• Staff trained in recognising and avoiding fire hazards. • Fire equipment maintained and checked on a regular basis. • Electrical items all professionally checked in line with H&S requirements. • H&S audit provides additional indication for risk avoidance. • A fire risk assessment is conducted as needed.	• Each Hospice building has a Fire Control Panel which automatically raises alarm and indicate area of fire. • A trained Fire Warden team has been established. • Fire extinguishers are located near the outer doors of all buildings, the type being appropriate to the location. • Fire drills are undertaken regularly. • 30 minute Fire Doors are installed throughout the site wherever needed.	2	3	6	Dir of IT & Est	Jan 24 / Apr 24
3	Gas leak	• A gas leak obviously constitutes a grave risk of fire or explosion and damage to health.	2	5	10	• All gas powered equipment and gas pipework is regularly tested for correct operation & absence of leaks		1	5	5	Dir of IT & Est	Jan 24 / Apr 24
4	Asbestos in building structures	• Asbestos within building structures has been outlawed for many years. Asbestos fibres present a serious risk to health when air borne.	2	4	8	• An Asbestos Management Plan is in place, which identifies the location of asbestos with the Hospice & charity shop buildings. Any work in one of these areas will require adherence to the management plan.		1	4	4	Dir of IT & Est	Jan 24 / Apr 24
5	Burst Pipe / Flood	• Water damage in any area can cause substantial damage to equipment, furniture, etc. Water near to electrical equipment can constitute a serious risk to staff.	2	4	8	• Regular maintenance and regular checks are undertaken.	• The location of all water pipes in all buildings is logged on appropriate building schematics. The location of all mains water shut off valves is also recorded. • Water main shut off valves are tested regularly to ensure that they operate correctly & have not seized up.	1	3	3	Dir of IT & Est	Jan 24 / Apr 24
6	Security / Break-in	• A security breach / break in can give rise to the theft of equipment, theft of data or risk to health of staff who may be present.	2	3	6	• All buildings have swipe card access control. Cards are only accepted where a staff member has been allowed access to that particular resource. • CCTV is installed in all buildings and charity / retail shops.		1	3	3	Dir of IT & Est	Jan 24 / Apr 24
7	Boiler / Heating System failure	• If the boiler or heating system develops a fault, it can represent a threat to health for both staff & patients during cold weather spells.	2	3	6	• The boiler & general heating system is monitored regularly to ensure correct operation.	• Several portable heating units are in store & available if required. • Ward rooms and several offices have air conditioning units that can provide heat.	1	2	2	Dir of IT & Est	Jan 24 / Apr 24
8	Oxygen Supply failure	• If the oxygen supply from St. Anthony's Hospital failed, no oxygen would be available for patients on-site.	1	4	4	• The oxygen supply pipes are checked regularly.	• Oxygen cylinders are kept on-site at St. Anthony's Hospital and can be brought into use immediately if the need arises.	1	2	2	Dir of IT & Est	Jan 24 / Apr 24

The axis for Likelihood should be from 1. Very Low – 2. Low – 3. Medium – 4. High – 5. Very High
The axis for Severity should be from 1. Light – 2. Serious – 3. Major – 4. Catastrophic – 5. Multi Catastrophic

Over 13 = red
8-13 = amber
7 or under = green