SINGLE CORPORATE SERVICES

DIGITAL SERVICES

Job title:	Technical Security Supervisor	***To be completed by HR*** *Job Reference Number* *2025/zzz*
Reporting to:	Technical Security Manager	
Accountable to:	Associate Director of IT	
Pay Band:	B7	

As part of the Single Corporate Service, this role provides a service across both Isle of Wight NHS Trust and Portsmouth Hospitals University NHS Trust.

The intention for the existing primary work locations to remain unchanged as there is no desire to change base locations unnecessarily. However, as the single corporate service will be delivered across both organisations, individuals may be required to undertake business travel from time to time. The staff mobility local agreement will apply.

For our leaders managing staff across multi-site locations, they will need to be visible and provide in person leadership. The arrangements and frequency will be agreed locally.

Job purpose

As team leader for the Technical Services Security Team, the postholder will be the lead IT Security technical role in the provision of effective, efficient and fully integrated IT operational services that maximise their availability and integrity for end-users and optimise the value gained by the Trust from its investment in IT. They will work across the Digital and the wider organisation to ensure that the Trust maintains the highest standards of compliance and defence against cyber security threats, ensuring that cyber security is a golden thread running through all of our processes and planning. This will be achieved by:

1. Oversee Security Operations: Ensure the smooth and efficient operation of security services across the Group Model across two hospitals, maintaining a safe and secure environment for patient and operational data.

2. Risk Assessment and Management: Conduct regular risk assessments in support of the Digital Service operations and working alongside the IT Security Architect for new services. Identifying potential security threats, and implementing appropriate measures to mitigate these risks in both hospitals.

3. Policy Implementation: support the development and adoption of hospital security policies and procedures, ensuring compliance with NHS guidelines and local regulations.

4. Staff Supervision and Training: Lead, train, and supervise Security team members , ensuring they are equipped with the skills and knowledge necessary to perform their duties effectively in a dual hospital setting.

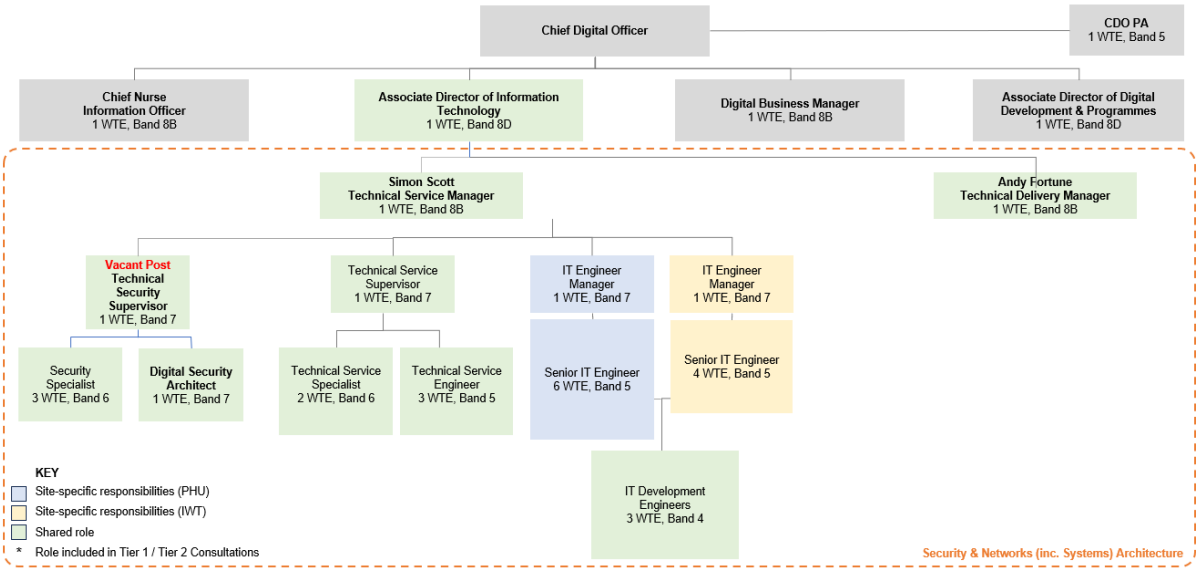
5. Incident Response Coordination: Coordinate and manage the response to security incidents, ensuring timely and effective resolution while minimizing disruption to hospital operations. Ensuring effective escalation communications are designed and implemented.

6. Technology and System Management: Oversee the maintenance and operation of security technology and systems, ensuring they are fully functional and up to date & as-one across both hospital sites.

7. Collaboration with Stakeholders: Work closely with Digital Service leadership members, clinical teams, and external partners to align security operations with the overall objectives of the Group Hospital Model.

8. Reporting and Documentation: Maintain accurate records of security incidents, audits, and inspections, and prepare detailed reports for digital & hospital management members to support decision-making and continuous improvement in security protocols.

Organisational Chart



Job summary

The Technical Security Supervisor will lead the Digital Cyber Security Team, helping to ensure the Confidentiality, Integrity and Availability of our infrastructure, systems and applications in line with established best practice, NCSC Cyber Assessment Framework, Data Security and Protection Toolkits and the Group Cyber Security Strategy.

Team Management

1. The postholder will report to the Technical Services Manager and is responsible for the management and day to day operation of the Cyber Security Team. Ensuring that tasks are appropriately prioritised and scheduled, skills appropriately utilised, procedures documented and followed, adequate coverage for absence and Out-of-Hours support is in place, and consistent, up-to-date documentation is established and maintained.

2. Provide the immediate line management for the Security Specialists and Information Security Architect within the Technical Security Team.

3. Monitor security standards for the Technical Services team, monitoring achievement against these, and devising improved ways of working, working with the Technical Services Manager.

4. As a team leader, take a lead role in the daily scrums held within the team to ensure the team collaboration and focus is aligned to the business outcomes.

5. Play a leading role in contributing to the Technical Services team working processes and operating procedures.

6. Facilitate Triage of incoming workloads and allocation of work throughout the team as required.

7. Ensure that Technical Services team and external contractors work in a responsible and safe manner and have due regard for health and safety regulations.

System Design & Hosting

8. Secure System Architecture: Working alongside the Digital Security Architect to design and implement robust security architectures for IT solutions, ensuring the integration of security principles such as least privilege, defence in depth, and secure by design throughout the IT solutions lifecycle.

9. Access Control Management: Develop and enforce access control policies, ensuring that only authorized personnel have access to sensitive systems and data, using multi-factor authentication, role-based access, and other security mechanisms.

10. Data Encryption and Protection: Implement strong encryption protocols and secure data handling practices to protect sensitive information both in transit and at rest, ensuring compliance with relevant regulations and standards.

11. Vulnerability Management: Conduct regular vulnerability assessments and security testing (e.g., penetration testing) to identify and mitigate potential security weaknesses in system design and hosting environments.

12. Incident Detection and Response: Design and implement systems for real-time monitoring and logging, enabling the timely detection, investigation, and response to security incidents and breaches.

13. Compliance and Audit Support: Ensure that systems are designed and hosted in accordance with relevant regulatory requirements and industry standards, providing necessary documentation and support during security audits and compliance assessments.

Software and Hardware Installation

14. Secure Configuration and Hardening: Ensure that all software and hardware installations follow secure configuration guidelines and hardening practices to minimize vulnerabilities and reduce the attack surface.

15. Patch Management: Oversee the timely installation of security patches and updates for both software and hardware across the entire IT landscape & two hospitals, ensuring that systems are protected against known threats and vulnerabilities.

16. Malware Protection: Implement and configure antivirus, anti-malware, and intrusion detection/prevention systems during installation to safeguard against malicious software and unauthorized access.

17. Access Control Implementation: Configure and enforce strict access controls during software and hardware installation, ensuring that only authorized users can access and modify system components.

18. Data Backup and Recovery Setup: Establish and verify secure data backup and recovery procedures during installation, ensuring that critical data is protected and can be restored in the event of a failure or breach.

19. Documentation and Compliance: Maintain detailed records of software and hardware installations, including configurations, security settings, and compliance with industry standards, to support ongoing security management and audits.

Infrastructure Developments/Innovation

20. Secure Infrastructure Design: Working with the Digital Security Architect to support the development of secure infrastructure solutions, incorporating advanced security measures and best practices into the planning, design, and implementation of new technologies.

21. Emerging Threat Mitigation: Proactively identify and address emerging security threats and vulnerabilities, adapting infrastructure developments to stay ahead of potential risks and ensure ongoing protection.

22. Integration of Security Technologies: Evaluate, select, and integrate cutting-edge security technologies and tools within the infrastructure to enhance overall security posture and support innovative solutions.

23. Scalability and Flexibility: Ensure that infrastructure developments are designed with scalability and flexibility in mind, allowing for secure expansion and adaptation to future technological advancements.

24. Automation and Orchestration: Implement automation and orchestration tools to streamline security processes within infrastructure developments, improving efficiency, consistency, and responsiveness to security incidents.

25. Collaboration with Stakeholders: Work closely with cross-functional teams, including IT, operations, and management, to align infrastructure innovations with security requirements and Hospital Group aims, ensuring that security is integrated into all phases of development.

Key Responsibilities

Communication and Working Relationships

- The role requires well developed communications and relationship management skills. Promote effective communication and networking with multi-disciplinary and multi-agency teams to ensure information security risks are well understood and managed, while developing a shared understanding of the pressures and priorities of partner organisations
- The post holder will provide face to face, written, verbal and electronic communications to a range of The Trust's managers and senior managers.
- The postholder is expected to present and communicate highly complex multi-stranded and sometimes contentious information about our networks and telephony estate, operational availability, security compliance and threat exposure levels.
- Preparing reports and helping to develop business cases to support future development.
- They will provide, receive and process complex, sensitive information; communicates complex Digital and corporate issues to non-digital managers; negotiates with external organisations over service issues. E.g third party suppliers, ICB
- Communicate in a manner that is consistent with relevant legislation, policies and procedures

Analytical and Judgement

- Identify and analyses information security risks within new and changed IT Infrastructure components and The Trust's applications.
- Investigate highly complex information security issues such as related to breaches of security, identify of architectural security solutions to resolve including resource requirements from within Digital and Information Governance.
- Escalate non-compliance security polices and standards to senior management, or project managers.
- The postholder will have to analyse highly complex facts and situations, responding in real time to emerging incidents, problems and service requests, interpreting and comparing a range of options.
- They will be responsible for managing change process and will need to monitor impact and be ready to respond if changes cause unexpected or adverse effects.
- They will be required to investigate and respond to security incidents and to ensure the security and integrity of Trust networks, and telephony.
- They will analyse and interpret complex problems or situations requiring analysis, interpretation, comparison of a range of options.
- Analyses complex problems relating service issues; makes judgements regarding allocation of resource for Digital work.

Planning and organising

- The postholder is required to plan and organise broad range of complex activities; formulates, adjusts plans or strategies Plans projects which impact across the department & organisation, delivery of Digital services for own area; contributes to medium term Digital strategy.
- They will oversee change management processes and ensure that appropriate remediation's are in place and tracked in response to a continually evolving cyber security landscape.
- They will be required to monitor system performance, design and scale infrastructure to respond to changing business requirements.
- Research and propose resilient solutions that meet the clinical and business need of the Trust.

Physical Skills

- Have advanced keyboard and computer skills in particular the use of function and other special keys and key combinations to control and program a range of computer equipment and network devices.

Patient Client Care

- The postholder will have occasional contact with patients and carers in a wide variety of situations (including mental health) during the course of their duties.
- They will Assist patients /clients during incidental contacts.

Policy and Service Development

- The postholder implements Digital policies and procedures for their own professional area.
- They are closely involved in the development and implementation of policy for Information systems, security and governance.
- They monitor and enforce policies that affect the security and integrity of the Trust's computer systems and network and ensure that legislation is not breached.

Financial Management

- The postholder will be a budget holder for their section.
- They will specify and select systems to monitor and enforce security across the Trust's network, telephony and security systems.
- Contracts will need to be reviewed to ensure they provide best value and broadest protection, within existing budget constraints.

Management/Leadership

- Responsible for the line management of a department
- Contributes, with input of the programme manager, to the development of more junior staff in understanding and use of security management methodology
- The postholder will be called upon to deliver training in network operation, management, security and troubleshooting to colleagues within the department and across the Trust.
- Line Management of IT Specialists with a focus on IT Operational Security and Patch Management
- Workload management and scheduling of IT Security Requests and Incidents, ensuring timely resolution in line with agreed SLAs
- Develop performance standards and objectives (SMART) for IT Operational Staff, monitoring achievement against these and devise improved methods of working
- Complete Performance appraisals of members of IT Operational staff, agreeing development needs and identifying and implementing appropriate training and development opportunities. Ensure that these contribute towards department and team objectives
- Ensure that IT Operational staff work in a responsible and safe manner in line with Trust and Departmental policies and procedures
- Participate in day-to-day event management to support the objectives of the larger IT Service Delivery Team
- Ensure IT Operational events are dealt with and responded to in a timely fashion and follow agreed SLAs and processes
- They are expected to maintain, refresh and continually develop their own skill set and knowledge.

- Ensure communications with all affected parties both internal to IT, to the Trust and relevant Third Parties are timely, accurate and informative

Information Resources

- Responsible for maintaining accurate records within the Trust's security and risk management systems, including regular highlight reporting, security planning, risk and issue management, and benefits identification.
- The postholder is responsible for ensuring the security, availability and integrity of our networks and telephony to deliver the Trust's corporate and clinical applications.
- They will manage and maintain multiple network and security systems as a major job responsibility.

Research and development

- Undertakes complex surveys/audits relating to security benefits.
- Benchmarking with other Trusts and exploring lessons learned
- The postholder will be required to assist in information collection, collation and presentation for audit, survey, research and reporting purposes.
- They will be responsible for performance and acceptance testing of our network and communications and regularly undertake testing to ensure effective operation of our disaster recovery and business continuity plans.
- Responsible for their own learning and development including identifying and researching any areas of learning that add to the knowledge base within the programme

Freedom to Act

- Full responsibility for the day-to-day management of security with freedom to act delegated from the Technical Service Manager.
- The postholder is expected to work under their own initiative, but within National guidelines, local policies and standard operating procedures.
- They will be expected to interpret how policies should be implemented within the service and wider organisation using their judgement and expert knowledge to ensure the best outcome for the organisation requirements and ensuring a sustainable service.
- They will be expected to research and seek guidance from other staff and departments as required.

Physical effort

- A combination of sitting, standing, and walking with little requirement for physical effort. There may be a requirement to exert light physical effort for short periods.
- There may be a requirement to exert light physical effort for short periods.

Mental effort

- There is a frequent requirement for concentration where the work pattern is predictable with few competing demands for attention, or there is an occasional requirement for concentration where the work pattern is unpredictable.

Emotional Effort

- Exposure to distressing or emotional circumstances is rare, or occasional indirect exposure to distressing or emotional circumstances.

Working conditions

- Requirements to use Visual Display Unit equipment more or less continuously on most days.

Person Specification

Criteria	Essential	Desirable	*How criteria will be assessed*
Qualifications	• ITIL v3 Foundation • Degree-level Qualification or equivalent in a Computing or analytical field • Technical Accreditation in one or more of the following: - ○ Microsoft MCP/MCSA/MCSE ○ Cisco CCNA ○ CompTIA Security+ ... ○ Certified Ethical Hacker (CEH) ...	**ISO27001** **CISSP**	**Application and Interview**
Experience	• Broad practical experience and 'Hands-on' technical experience in the majority of the following: - ○ Microsoft Windows and BackOffice Servers (SQL Server, Exchange) ○ App-V or alternate Application Virtualisation solution ○ Citrix XenApp ○ Cisco Switches and ASA and general networking ○ SAN technologies (Block and File) ○ AppSense		**Application and Interview**

	○ VMware/Server Virtualisation ○ Security Event Monitoring/Aggregation ○ Event Monitoring solutions (e.g. Solarwinds/Zabbix or similar)		
Knowledge	• Demonstrable in depth understanding of current NHS standards and policies relating to security • Ability to manage multiple complex projects to a successful conclusion, using structured methodologies • Substantial knowledge of Change Management processes and techniques • Working to IT service management best practice i.e. ITIL • Ability to forge long-term working partnerships with individuals and groups from internal and external departments and organisations • Ability to write clear concise reports, letters, minutes and documents using a good standard of English • Excellent organisational, problem solving, communication and analytical skills • The ability to tackle highly complex issues and resolve them to the benefit of the service. • The ability to remain current with emerging technologies • Sensible negotiator with practical expectation of what can be achieved		**Application and Interview**

Compliance statement to expected organisational standards.

To comply with all Trust Policies and Procedure, with particular regard to

- Risk Management
- Health and Safety

- Confidentiality
- Data Quality
- Freedom of Information
- Equality Diversity and Inclusion
- Promoting Dignity at Work by raising concerns about bullying and harassment
- Information and Security Management and Information Governance
- Counter Fraud and Bribery

The Trust has designated the prevention and control of healthcare associated infection (HCAI) as a core patient safety issue. As part of the duty of care to patients, all staff are expected to: Understand duty to adhere to policies and protocols applicable to infection prevention and control.

- Comply with key clinical care policies and protocols for prevention and control of infection at all time; this includes compliance with Trust policies for hand hygiene, standards (universal) infection precautions and safe handling and disposal of sharps.
- All staff should be aware of the Trust's Infection Control policies and other key clinical policies relevant to their work and how to access them.
- All staff will be expected to attend prevention and infection control training, teaching and updates (induction and mandatory teacher) as appropriate for their area of work, and be able to provide evidence of this at appraisal.

- To perform your duties to the highest standard with particular regard to effective and efficient use of resources, maintaining quality and contributing to improvements.

- Ensure you work towards the Knowledge and Skills Framework (KSF) requirements of this post. KSF is a competency framework that describes the knowledge and skills necessary for the post in order to deliver a quality service.

- Your behaviour will demonstrate the values and vision of the Trust by showing you care for others, that you act professionally as part of a team and that you will continually seek to innovate and improve. Our vision, values and behaviours have been designed to ensure that everyone is clear about expected behaviours and desired ways of working in addition to the professional and clinical requirements of their roles.

- Ensure you adhere to and work within local and national safeguarding children legislation and policies including the Children Act 1989 & 2004 , Working Together to Safeguard Children 2013, 4LSCB guidance and the IOW Safeguarding Policy.

- Ensure you adhere to and work within the local Multiagency safeguarding vulnerable adults policies and procedures

- Ensure that you comply with the Mental Capacity Act and its Code of Practice when working with adults who may be unable to make decisions for themselves,

- Ensure that you maintain personal and professional development to meet the changing demands of the job, participate in appropriate training activities and encourage and support staff development and training.
- Respect the confidentiality of all matters that they may learn relating to their employment and other members of staff. All staff are expected to respect conform to the requirements of the Data Protection Act 1998, including the responsibility to ensure that personal data is accurate and kept up to date

- If your employment is to a post that requires you to be registered with a professional body, the continuation of your employment is conditional upon you continuing to be registered with the appropriate professional body. The Trust will require evidence of current registration.

- Proactively, meaningfully and consistently demonstrate the Trust Values in your every day practice, decision making and interactions with patients and colleagues.

- Perform any other duties that may be required from time to time.

- Contribute to the IT Departments on-call rota and if required, maintain required skills, experience and resource levels allowing for hospital digital 24/7 services.

This job description may be altered, from time to time, to meet changing needs of the service, and will be reviewed in consultation with the post holder.