
Job Description for IT Security Network Administrator

Responsible to: Trust IT Manager

Based at: New College Pontefract, travelling to sites when required.

The successful experienced candidate will join the NCLT IT Services Department helping to provide a robust level of network security for all users whilst delivering a cyber secure and safe network.

OVERALL PURPOSE OF THE POST

Provide cyber security expertise using strong analytical problem-solving skills and a high degree of initiative and dependability in order to strengthen the Trust's network security.

Monitor and analyse the network security, assessing alarms and pre-empting issues using cyber security tools and devices.

Ensure that the IT services and equipment are deployed in line with the Trust's policies and vision for IT and assisting the Trust IT Manager in creating a robust, secure and efficient network.

MAIN DUTIES

- To monitor NCLT network systems, detect security threats (events), analyse and assess alarms, report on threats, intrusion attempts and false alarms, either resolving or escalating issues.
- Administer information security software controls.
- Administer processes for discovering vulnerabilities in network systems.
- Prevent, detect and respond to threats with Azure Security and compliance.
- Identify potential weaknesses and implement measures in collaboration with the Network Administrators and Trust IT Manager.
- Implement and monitor NAT.
- Proactively Investigate Security information and Event Management (SIEM) and network logs for potential issues.
- Support new security projects and initiatives.
- Daily network security monitoring, implementing required changes alongside on the Trust IT Manager.
- Maintain Network Access Control, ensuring restrictions are in place for authorised devices and compliant policies.
- Set up of NCLT penetration testing, investigating and resolving issues identified.
- Monitor and analyse broadcast traffic.
- Work as part of a team to improve resilience of the current network environment.
- Maximise network performance by monitoring performance, troubleshooting network problems and outages, scheduling upgrades and collaborating with network architects on network optimisation alongside the Trust IT Manager.
- Undertake data network fault investigations in local and wide area environments, using information from multiple sources.
- Secure network systems by establishing and enforcing policies, and defining and monitoring access.
- The configuration, support and administration of firewall environments in line with IT security policy.

- Update job knowledge by participating in educational opportunities, reading professional publications, maintaining personal networks and participating in professional organisations.
- Report network operational status by gathering and prioritising information.
- Upgrade data network equipment to the latest stable firmware releases.
- The configuration of routing and switching equipment.
- Remote support of on-site engineers and end users during installation.
- Capacity management and audit of IP addressing and hosted devices within the network.
- Working alongside the Trust IT Manager to liaise with project management teams, third-line engineers and service desk engineers on a regular basis.
- First point of support contact for junior IT Technicians and supporting IT Technicians' training (first and second line).
- Supporting staff and students within the Trust when required (first and second line).
- Ensure that hardware and upgraded software are deployed and maintained in accordance with the requirements of the Trust's strategic vision for IT.
- Assist the Trust IT Manager to develop an effective, resilient and scalable LAN for the Trust.
- Support current Trust systems, Cisco switches, HP Switches, WIFI.
- Be aware of, advise on, and implement Health and Safety and Equal Opportunities policies within the IT Support area and liaise with the Trust IT Manager and/or Health and Safety Manager as appropriate.
- Undertake other duties as reasonably requested commensurate with the grade of the post.

There is an expectation across the Trust that all support functions will work together and support each other as and when required.

This job description is subject to amendment, from time to time, within the terms of your conditions of employment, but only to the extent consistent with the needs of the college/trust, and only after consultation with you.

All staff and senior post holders have a duty for safeguarding and promoting the welfare of young people. Staff must be aware of the college procedures for raising concerns about students' welfare and must report any concern to the designated officers without delay. Staff must also ensure that they attend the appropriate level of safeguarding training identified by the college as relevant to their role.

The post holder's duties must at all times be carried out in compliance with the Trust's Equality and Diversity Policy, and the post holder must take reasonable care of the health and safety of self, other persons and resources whilst at work. This entails supporting the Trust's responsibilities under the Health and Safety Act.

All staff are expected to support the achievement of the Trust/college's mission and strategic objectives and to demonstrate its values through their behaviour.

Person Specification for IT Security Network Administrator

There will be various opportunities for you to demonstrate you have the necessary attributes for this role such as through completion of the application form, at interview, during any tasks and through your provided references.

ATTRIBUTES	ESSENTIAL	DESIREABLE
Relevant Experience	<ul style="list-style-type: none"> • Experience of cybersecurity monitoring • Experience in the support and management of Windows servers/2016/2019 • Strong understanding of network infrastructure and network hardware. • Network Security experience, monitoring network performance. • Previous experience with SEIM or service desk toolsets. 	<ul style="list-style-type: none"> • Knowledge of Sophos UTM, FortiGate, Sophos Central, AV, Meraki switching, HP Switching, VMware, Linux, VOIP phone Systems, MAC Environments, DEP. • Experience using advanced tools to determine vulnerabilities. • Experience of Active Directory, DHCP, DNS, TCP/IP, Firewalls, Group Policy. • Experience working with O365, Azure Administration.
Education and Training	<ul style="list-style-type: none"> • Cyber security training, working knowledge of Cyber Essentials and ICT security architectures and common designs for mitigation information security risks. • Excellent IT skills including knowledge of computer networks, operating systems hardware, security. • Good general standard of education, including a minimum of GCSE equivalent in Maths and English at Grade C or above. • Well-developed oral, written and interpersonal skills. 	<ul style="list-style-type: none"> • 5 years' experience in security systems .
Special Skills and Knowledge	<ul style="list-style-type: none"> • Working knowledge of Cyber Essentials and ICT security architectures and common designs for mitigation information security risks • Keep up to date with the latest security technology developments, • Familiarity with multiple programming and scripting languages, java, C/C, Ruby, Python etc. • Familiarity TCP/IP, IPSEC, HTTP, HTTPS, routing protocols. • Experience working with O365, Azure Administration. • Experience investigating network logs for anomalies in order to identify suspicious behaviour. • Analytical and problem-solving skills to identify and assess risks. • Good time management and organisational skills. • Ability to communicate at all levels. • Ability to maintain high standards whilst working quickly. • Experience of working unsupervised. • Troubleshooting diagnosing and resolving hardware and software problems. • Ability to gather relevant information about a support issue from non-technical staff/students. 	
Personal Skills and Qualities	<ul style="list-style-type: none"> • Experience of working effectively as part of a team. • Experience of prioritising work under pressure. • Enthusiasm for the role. • Planned approach to own and work of others. 	

Additional Factors	<ul style="list-style-type: none">• Commitment to continuous improvement and willingness to learn from experience.• Commitment to equal opportunities, health and safety and safeguarding.	<ul style="list-style-type: none">• Desire to work in an educational institution with people in the 16-19 age range.
---------------------------	---	--