UNIVERSITY of BRADFORD

Job Description

Network and Security Engineer

Directorate of Infrastructure

Brief summary of the role

Role title:	Network and Security Engineer
Grade:	8
Faculty or Directorate:	Infrastructure
Service or Department:	IT Services
Location:	Main Campus
Reports to:	Head of Networks and Security
Responsible for:	
Work pattern:	

About the University of Bradford

Values

At the University of Bradford, we are guided by our core values of Excellence, Trust, Innovation, and Inclusion. These values shape our approach and our commitment to making diversity, equity, and inclusion part of everything we do – from how we build our curriculum to how we build our workforce. It is the responsibility of every employee to uphold the university values.

Equality, Diversity, and Inclusion (EDI)

We foster a work environment that's inclusive as well as diverse, where staff can be themselves and have the support and adjustments to be successful within their role.

We are dedicated to promoting equality and inclusivity throughout the university and have established several networks where individuals can find support and safe places fostering a sense of belonging and acceptance. We are committed to several equality charters such as Athena Swan, Race Equality Charter, Disability Confident and Stonewall University Champions Programme.

Health, safety, and wellbeing

Health and Safety is a partnership between employee and employer each having responsibilities, as such all employees of the University have a statutory duty of care for their own personal safety and that of others who may be affected by their acts or omissions.

It is the responsibility of all employees that they fulfil a proactive role towards the management of risk in all of their actions. This entails the risk assessment of all situations, the taking of appropriate actions and reporting of all incidents, near misses and hazards.

Managers should note they have a duty of care towards any staff they manage; academic staff also have a duty of care towards students.

All colleagues will need to ensure you are familiar with any relevant Health and Safety policies and procedures, seeking advice from the Central University Health and Safety team as appropriate.

We are registered members of the University Mental Health Charter. This visibly demonstrates our commitment to achieving cultural change in student and staff mental health and wellbeing across the whole university, whilst supporting the vision of our People Strategy to create a culture and environment of transformational diversity, inclusion and social mobility, creating a place where our values come to life and are evident in our approach.

Information governance

Employees have a responsibility for the information and records (including student, health, financial and administrative records) that are gathered or used as part of their work undertaken for the University.

An employee must consult their manager if they have any doubts about the appropriate handling of the information and records with which they work.

All employees must always adhere to data protection legislation and the University's policies and procedures in relation to information governance and information security.

Employees will be required, when and where appropriate to the role, to comply with the processing of requests under the Freedom of Information Act 2000.

Criminal record disclosures and working with vulnerable groups

Depending on the defined nature of your work and specialist area of expertise, the University may obtain a standard or enhanced disclosure through the Disclosure and Barring Service (DBS) under the Rehabilitation of Offenders Act 1974.

All employees of the University who have contact with children, young people, vulnerable adults, service users and their families must familiarise themselves, be aware of their responsibilities and adhere to the University's policy and Safeguarding Vulnerable Groups Act 2006.

The University is committed to protect and safeguard children, young people and Vulnerable Adults.

Suitable applicants will not be refused positions because of criminal record information or other information declared, where it has no bearing on the role (for which you are applying) and no risks have been identified against the duties you would be expected to perform as part of that role.

Role holder: essential and desirable attributes

Qualifications

Essential	Educated to degree level in IT related subject or equivalent relevant experience. ITIL V3 Foundation or equivalent relevant experience.
Desirable	Vendor accredited - CCNP or equivalent.

Experience, skills, and knowledge

Essential	Knowledge of IP networks and fault finding. Good knowledge of Data Networking protocols including TCP/IP, OSPF, DHCP,DNS. Have good experience of firewalls, penetration testing tools and techniques, and security incident management. Knowledge and experience of switch, router, and firewall/security products. Knowledge and experience of LAN and WAN technologies. Understand and develop the key concepts, elements, and objectives of the University security program. Understand the relationships between key security controls (policies, anti-malware, anti- virus, firewalls, etc.) and the risks they mitigate.

	Knowledge of Microsoft and Linux based operating systems. Ability to be creative in problem solving. Understanding of potential damage to systems, data, and reputation by non- adherence to basic security principles.
Desirable	Experience of working within the higher education sector or other public sector environment. Experience of other non-Windows server operating systems, Solaris, Unix etc. IT Security or Networking industry recognised qualifications (CCNA, ISC, GPEN etc Experience of virtual networking, VSphere, Hyper-V, NSX etc

Personal Attributes

Essential	A clear commitment to provide an excellent University wide customer experience. Ability to communicate well at all levels and ability to work alone and as part of a team. Ability to take ownership and manage incidents and projects from conception to closure. Ability to solve logical problems, with experience of network and infrastructure systems issues.

Main purpose of the role

Manage the day-to-day support and administration of the University Network system components.
Proactively monitor security of University IT systems to detect issues and possible breaches.
Responsible for smooth operation of University's network infrastructure.

Main duties and responsibilities

1. Use network and security management tools to monitor the performance of IT infrastructure systems, services and components in relation to their availability, performance and security
2. Identify operational problems and contribute to their resolution, including liaising with hardware, software and service suppliers to resolve problem.
3. Perform agreed operational procedures, including back-up and recovery operations, infrastructure component installation, configuration and maintenance, management of network address space.
4. Contribute to the design, development and implementation of upgrades to the network and security infrastructure.
5. Liaise with the Infrastructure team with regards to the design, planning and implementation of upgrades to existing services and deployment of new services.
6. Taking an active role in procurement and deployment of security and network infrastructure and services.
7. Provide technical expertise, advice and guidance to staff at all levels across the University in aspects of Information Security & Networking. Provide training and technical documentation as required.
8. To act as a contributor in projects and working groups, to share expertise with colleagues and others.
9. Maintain expertise in Information Security through networking and liaison with external specialists and build collaborative links to facilitate information sharing.
10. Be a technical contact for information security incidents, liaising with outside parties as appropriate including JISC, CSIRT and other relevant third parties.
11. Assist with internal investigations as required by senior management.
12. Keep detailed records of security incidents, track relevant metrics and report on these as required.

13. Contribute to an internal penetration testing service, conducting technical tests and determining follow-up actions.
14. Produce and maintain technical documentation of supported services including standard operating procedures for service start-up, operation and shut-down.
15. Identify and document service support requirements of new network and security components.
16. Working effectively with others (both customers and within the IT Services teams) to extract requirements, timescales and developing appropriate technical responses.
17. Maintain personal credibility and authority to consult, influence and negotiate with colleagues and stakeholders at all levels.
18. Contribute to investigating and evaluating new technologies or upgrades to existing technologies to identify and implement solutions that will increase the security of the University's IT systems and data.

This document outlines the duties required at the current time to indicate the level of responsibility. It is not a comprehensive or exhaustive list and may vary to include other reasonable requests as directed by University management which do not change the general character of the job, or the level of responsibility entailed.