IT Services

Senior IT Services Specialist - Windows Endpoint Security

Job Ref: REQ250765

As part of the University's ongoing commitment to redeployment, please note that this vacancy may be withdrawn at any stage of the recruitment process if a suitable redeployee is identified.

School/Department Summary

IT Services is based in Holywell Park, a beautiful area of green campus with a large car park, good public transport links and next to Burleigh Woods. Loughborough IT came top in the National Student Survey for IT resources & facilities in supporting learning for several years in a row.

We have an incredibly supportive culture, an understanding of work/life balance, with hybrid working available. Staff particularly enjoy the flexibility available and the opportunity to contribute to interesting University wide projects. Colleagues have a wide variety of backgrounds from different areas, bringing a broad range of experiences.

Training is encouraged via secondment opportunities, lots of internal courses run by Organisational Development, job shadow, as well as online learning and external providers. Departmental lunches allow us to get together to meet all colleagues in person on a regular basis, in an informal setting.

Benefits

The University offers a wide range of employee benefits which can be found here.

We also offer an on-campus nursery with subsidised places, subsidised places at local holiday clubs and a childcare voucher scheme (further details are available at: http://www.lboro.ac.uk/services/hr/a-z/childcare-information---page.html

In addition, the University is supportive, wherever possible, of flexible working arrangements.
We also strive to create a culture that supports equity and celebrates diversity throughout the campus. The University holds a Bronze Athena SWAN award which recognises the importance of support for women at all stages of their academic career. For further information on Athena SWAN see http://www.lboro.ac.uk/services/hr/athena-swan/

Job Description

Job Grade: Management and Specialist, Grade 7

Job Purpose

To provide expert level technical knowledge and skills in the development and support of IT Services, End User Environment services. The primary focus for this job will be to ensure the EUE led services are secure. This will include working closely with the IT Security team and other teams across the department.

The role holder will need to lead on the deployment, monitoring, and reporting on all aspects of Endpoint security including the uptake of OS deployments, firmware, drivers, and encryption levels.

Additional key tasks associated with the role include, but are not limited to Vulnerability Management, Operating System deployments, image creation, automating tasks via scripting and deploying applications centrally.

The role holder will also have an excellent working knowledge of Microsoft Endpoint Configuration Manager and Microsoft Intune used to manage the current Windows 10 and 11 services. An excellent working knowledge of Active Directory, Group Policy, and Entra ID will help to create a modern and secure desktop environment.

Working as part of the End User Environment team, the post holder will collaborate with colleagues in IT Services and across the University and will be engaged in a varied set of projects and initiatives. This role will need to proactively build effective working relationships within the IT Platform teams, with IT Security, and across the University.

Job Duties

- To work closely with the departmental IT Security team and additional teams across the department to ensure end user environment services are secure. This will involve creating bespoke reports from within Intune and Configuration Endpoint Manager and creating processes to capture and remediate any insecure devices.
- Deploy Windows 10 and Windows 11 security patching from within Configuration Endpoint Manager and Intune. Ensure endpoints are secure and remediate any issues. Work with relevant support teams, as necessary.
- Lead on results from Security Penetration testing against the EUE services and ensure issues are remediated.
- Work with the Configuration Manager and Intune lead on creating and improving security reporting and associated process.
- Lead on technical features such as BitLocker, AppLocker, Laps, Windows feature, and driver updates.
- Work closely with the IT Security team and team colleagues to assess the server security vulnerability management reports desktop security scanning reports.
- Undertake a leading role in making sure all of our services are security compliant and work closely with the CESRN lead to ensure all CESRN service requirements are met.
- To be the backup for technical features including, but not limited to, supporting the Cyber Essentials certifications, Impero support and Task Sequence creation.
- Integrate with the well-established team and work cohesively across the department to support projects and services including training and mentoring colleagues in your technical speciality.
- To lead on the yearly image creation process used for the annual teaching computer labs refresh project. This will include an assessment of lessons learned from the previous year with specific consideration given to whether it met the users' needs. This task needs strict attention to detail and detailed documentation. It will also involve training support staff on how to image labs. This task will include coaching a technical backup for the role.
- Provide innovative solutions to meet requirements or address problems and convince others of the argument for change.
- Communicate technical and procedural changes to non-technical people, and ensure they understood the change and business impact. Build strong working relationships with colleagues outside of your team/department.

- Develop and maintain knowledge of the technical specialism by, for example, reading relevant literature, attending conferences and seminars, meeting and maintaining contact with others.

- Involved in the technical specialism through participating in national and regional events provided by UCISA, JISC, etc as appropriate.

- Be familiar with relevant University procedures and policies (EDI, acceptable use, data protection, freedom of information, information security, purchasing etc) and advise colleagues and end-users accordingly.

- Is responsible for service improvements and projects relating to technical expertise. This includes working with stakeholders to analyse and understand requirements, contribute technical content, and work to provide innovative IT solutions. This includes the management and co-ordination of consultants and contractors working in support of the responsibilities of the team, as necessary.

- Participate in projects, working across the University, to plan and develop new technical platforms for IT services and to roll out these services to users. In designing and delivering IT services, IT Services Specialists will consult with customers to understand and analyse their requirements, contribute technical content, and work to provide innovative IT solutions to support business critical University functions.

- Ensure that operational documentation for relevant systems, software, and products is fit for purpose and current. Provide advice and guidance to other colleagues and support staff on the correct and effective use of systems and software.

- Investigate potential and actual service problems and recommend solutions. Develop and use formal procedures to plan and evaluate proposed solutions. Develop and use procedures for collection of critical information in the event of system software failure. Analyse documentation, storage dumps and logs relating to system software failures to identify the failing component. Isolate failures and recommends actions to circumvent problems and enable the restoration of services with the minimum of business impact. Consults with suppliers to obtain corrective code, installing and evaluating the code to ensure a permanent resolution.

- Contributes to the implementation of service continuity measures which include: the development of Service Recovery Plans, system backup processes, testing of system recovery, system cloning for development and testing purposes. This includes providing advice for Business Continuity scenario planning.

- To support the team as senior technical support lead, dealing with technical issues escalated by colleagues for support and guidance.

- Responsible for supporting other members of the department, ensuring they adhere to best practices with the management tools.

- Provide expert-level support and guidance for issues escalated from other teams and colleagues.

- The role will be the principal design authority for the services within their specific technical and management specialisms. This includes developing mutually agreed service roadmaps; whilst articulating the importance of following good service management and information security practice.

- Stay updated on emerging technologies, IT Security and wider industry trends and share knowledge to others managing or delivering endpoint services.

- Writes, or contributes to, articles, and papers and speaks at conferences, user groups, or specialist subject groups on topics involving the technical specialism. Plays a leading role in special interest groups concerned with the technical specialism. Is fluent at articulating best practice and is a recognised authority in the technical specialism.

- Undertake various other tasks on an occasional basis at the request of more senior staff in the professional service, and to a level commensurate with training, knowledge, grade, and skills.

Note: This job description was created in the spirit of the BCS (The Chartered Institute for IT), SFIA (Skills for the Information Age) level 5 and 6 with support from the BCS

IT Services Special Conditions:

This post involves configuration, development, or management of infrastructure for corporate IT systems or carrying out other work that requires privileged access to applications and data. Therefore, applicants must provide details of referees including their current line manager covering the three years prior to their application to a post at the University.

Many staff carry mobile phones which allow them to be notified by various systems at all reasonable hours of the week. When monitoring, diagnosis and configuration of services needs to be done outside normal working hours, it can sometimes be appropriate for the work to be carried out remotely at home when convenient.

Attendance on site outside normal working hours is occasionally necessary, for example during major system changes and maintenance. Such out-of-hours working as is necessary is scheduled in negotiation with the group of staff with relevant skills and takes account of the personal commitments and wishes of colleagues.

For purposes of system management, IT Services staff often have enhanced access to data, files and computer systems and must always respect the privacy of information to which they have enhanced access. The only exception to this will be investigations authorised by IT Services Director or their nominee.

Points To Note

The purpose of this job description is to indicate the general level of duties and responsibility of the post. The detailed duties may vary from time to time without changing the general character or level of responsibility entailed.

Special Conditions

All staff have a statutory responsibility to take reasonable care of themselves, others, and the environment and to prevent harm by their acts or omissions. All staff are therefore required to adhere to the University's Health, Safety and Environmental Policy & Procedures.

All staff should hold a duty and commitment to observing the University's Equity & Diversity policy and procedures at all times. Duties must be carried out in accordance with relevant Equity & Diversity legislation and University policies/procedures.

Successful completion of probation will be dependent on attendance at the University's mandatory courses which include Respecting Diversity and, where appropriate, Recruitment and Selection.

Organisational Responsibility

Reports to End User Environment Team Manager but may receive strategic instructions from the Head of IT Platforms.

Person Specification

Your application will be reviewed against the Essential and Desirable criteria only which listed below. Applicants are strongly advised to explicitly state and provide evidence on how they meet each of these criteria in their application. A CV will not be used to evaluate your application.

You may be assessed on answers to interview questions not directly listed in the Essential and Desirable criteria but pertain to skills related to the role.

It may be helpful to structure this like below:

[EC1, EC2, DC2] Previous experience that demonstrates how you meet these criteria.

Stages of assessment are as follows:

1 – Application
2 – Technical Interview/Assessment
3 – Second Interview

Essential Criteria

Area	Criteria	Stage
	[EC1] Expertise in the deployment, management, reporting, and remediation of Microsoft security updates to MS Windows endpoints via Microsoft Endpoint Configuration Manager.	1,2
	[EC2] Expertise in the deployment, management, and remediation of Microsoft security updates to MS Windows endpoints via WuFB within Microsoft Intune.	1,2
	[EC3] Experience in Client Health reporting and security monitoring on a managed Windows service via Configuration Manager and Intune	1,2
	[EC5] Expertise in the creation of MS Operating system images and deployments using Configuration Manager.	1,2
	[EC6] Hands on direct experience of centrally managing endpoints using the management tools used by the team, which includes Configuration Manager, Intune, Active Directory and Group Policy.	1,2
	[EC7] Experience of packaging applications and deploying via Configuration Manager and Intune.	1,2
	[EC8] Experience in supporting large corporate systems and applications in an enterprise networked environment.	1,2
	[EC9] Experience of managing projects and service improvements.	1,3
Skills and abilities	[EC10] Excellent logical diagnostic skills demonstrated by the ability to troubleshoot and resolve complex technical issues on Windows operating systems.	1,2
	[EC11] Ability to undertake security vulnerability scanning, explain the associated service risk, and resolve identified security issues	1,2
	[EC12] Ability to use scripting languages such as, PowerShell, to automate tasks within a Microsoft Windows environment.	1,2
Training	[EC13] Demonstrate evidence of proactively undertaking your own professional development.	1,2
Qualifications	[EC14] Degree combined with relevant professional IT qualifications and experience. OR alternative qualifications and experience.	1

Desirable Criteria

Area	Criteria	Stage
Skills and abilities	[DC1] Experience of using DevOps style processes e.g. Code Versioning, Continuous Integration, and automation to manage infrastructure/platform services.	1,2
	[DC2] Ability to gather detailed information from Microsoft Intune via APIs to produce endpoint reporting	1,2
	[DC3] Working knowledge of IT/Information Security standards and frameworks such as Cyber Essentials	1,2
	[DC4] Experience in Client Health reporting and security monitoring on a managed Windows service via Configuration Manager and Intune	1,2
	[DC5] Experience with Cyber Essentials and Cyber Essentials Plus certifications	1
Qualifications	[DC6] ITIL Foundation qualification or training.	1

Conditions of Service

The position is Full-time and Open-ended. Salary will be on Management and Specialist Grade 7, £46,735 – £55,755 per annum, at a starting salary to be confirmed on offer of appointment.

The appointment will be subject to the University's Terms and Conditions of Employment for STAFF GRADES 1-5/STAFF GRADES 6 AND ABOVE, details of which can be found here.

The University is committed to enabling staff to maintain a healthy work-home balance and has a number of family-friendly policies which can be found here.

Applications

The closing date for receipt of applications is 22 September 2025.