Job Description

IT Officer (Systems Administrator)

Summary

SOCIT is an Information Services team that provides IT services to a Consortium of Oxford Colleges. The IT Officer is part of the SOCIT team; specifically, part of a small team of IT Officers managing, monitoring, maintaining and automating the systems for all the SOCIT colleges, providing 2nd and 3rd line support for the support team, and providing high level technical input to projects.

The job-holder reports to the Head of Infrastructure and must possess strong networking and system administration skills, having a background in this area to serve various business needs. The post-holder is confidently able to develop and recommend new systems using the latest technologies. Documentation and Knowledge sharing is encouraged within the team.

The role specialises in several areas, networking, VMware virtualization and has good knowledge of Windows/Linux server and database management, scripting and security.

System Administration:

Server Management

- Manage and maintain server infrastructure across Windows and Linux environments.
- Ensure high availability, performance, and reliability of all server systems.

System Updates & Patching

- Perform regular updates, patching, and security maintenance for Windows and Linux servers.
- Monitor systems to ensure compliance with security and update policies.

Network Infrastructure

- Design, implement, and maintain enterprise-level wired and wireless network infrastructure.
- Ensure optimal performance, scalability, and resilience of network systems.

Troubleshooting & Support

- Diagnose and resolve hardware, software, and network-related issues.
- Provide second and third-line technical support for users and systems.

User & Access Management

- Administer user accounts, permissions, and access controls in line with organisational policies.

Infrastructure Maintenance & Enhancement

- Maintain, enhance, and upgrade overall IT infrastructure, including servers and network components.
- Ensure systems remain secure, efficient, and up to date.

Hardware & Software Deployment

- Install, configure, and maintain server hardware and system software.
- Roll out new server hardware as required.

Upgrades & Planning

- Organise, plan, and execute system, network, and firewall upgrades.

Documentation

- Develop and maintain comprehensive technical documentation for systems, processes, and procedures.

Technical Advisory

- Provide expert advice on system-related matters.
- Maintain up-to-date knowledge of industry standard, technologies, and best practices.

Disaster Recovery & Business Continuity

- Support disaster recovery and business continuity planning, including backup strategies, testing, and documentation.
- Assist in the development and execution of recovery procedures to ensure minimal service disruption in the event of system failures or incidents.

Support

Advanced Technical Support

- Provide second- and third-line support to the helpdesk support team.
- Deliver high-level technical input and expertise to infrastructure and IT projects.

General IT Support

- Offer technical support and guidance to staff and students during peak periods or as required.

Active Directory & Identity Services

- Administer and manage Active Directory services, including user accounts, group policies, and access control.
- Support and maintain authentication systems, including intranet and web-based SSO solutions (e.g. Shibboleth).

Security & System Hardening:

- Implement and maintain security best practices across all Unix-based systems.
- Regularly apply patches and updates to operating systems and applications to mitigate vulnerabilities.
- Monitor system logs and alerts for suspicious activities and perform incident response when necessary.
- Conduct security audits and vulnerability assessments to identify and remediate potential risks.

Collaboration & Support:

- Provide technical support to users, helping with server-related issues, research software deployments, and best practices.
- Collaborate with research teams to understand infrastructure needs and assist in the setup of environments and services.

Cybersecurity & Risk Management

- Contribute to the prevention of malware, virus infections, and security breaches through proactive system management and patching.
- Monitor, assess, and report on vulnerabilities and risks associated with known exploits.
- Support the implementation of security best practices and protective technologies.

Security & System Hardening:

- Implement and maintain security best practices across all
- Monitor system logs and alerts for suspicious activities and perform incident response when necessary.
- Enforce access control policies and implement system hardening measures to protect sensitive data.

Experience

Essential Skills:

- Extensive experience managing IT systems and teams within a service-oriented environment.
- Proven experience as a Systems Administrator, Network Administrator, or in a similar role.
- Strong administrative experience with VMware or equivalent virtualised server environments.
- Significant hands-on experience in advanced system administration across Windows and/or Linux in complex, large-scale environments.

- Strong knowledge of TCP/IP networking, including routing, switching, firewall configuration, and network security.
- Practical experience implementing security best practices and tools, such as firewalls and intrusion detection/prevention systems.
- Strong communication and problem-solving abilities.
- Ability to prioritise workloads effectively and perform under pressure.
- Ability to work both independently and collaboratively as part of a team.

Desired Skills:

- Relevant professional certifications (e.g. CompTIA Network+, CompTIA Security+, MCSE, CCNA).
- Experience with scripting and automation using languages such as PowerShell, Python, or Bash.
- Knowledge of containerisation technologies (e.g. Docker, Kubernetes).
- Experience with database administration (e.g. SQL, MySQL).
- Familiarity with ITIL principles and best practices.
- Experience with system monitoring and security tools (e.g. Wazuh, Zabbix).
- Understanding of disaster recovery and business continuity planning.