Senior Infrastructure Security Officer

Full time, 37 Hours per Week
£35,314 – £43,113 per annum
Andover / Winchester

This is an excellent opportunity to join a dynamic, forward thinking IT Shared Service as a cyber-security professional.

The purpose of this role is to manage and maintain the ITIL Security Management Information System (SMIS) which protects all IT services including users, applications and hardware against cyber and security threats.

As part of the Operations Team you will deliver a secure and operational IT Infrastructure to meet agreed performance indicators and service level agreements.

Reporting to the Operations Manager, this challenging post provides the opportunity to play a key role in the influencing of the IT security standards for the shared service.

Key responsibilities:

- Research and promote the latest security trends and manage the implementation of solutions.
- Daily risk management of security threats.
- Delivery of all IT digital security strategies and associated policies and procedures.
- Provide project management to implement new and existing technologies.
- As part of a team provide support in all aspects of network and infrastructure management.

Required skills:

- Educated to Degree level / equivalent formal IT security qualification or equivalent experience.
- Proven knowledge of PSN and PCI compliance.
- Strong technical skills in System Architecture, Networking, Virtualisation, Storage, Hardware.
- Prior experience of delivering IT compliance policies and procedures.
- In-depth knowledge of security protocols, best practice and risk management.

Test Valley Borough Council and Winchester City Council are committed to developing staff though training and promote a strong work life balance. We also offer a number of benefits including free on-site parking, generous leave entitlements, pension scheme and an on-site restaurant.

For an informal discussion about the post please contact Nicky Richards, Operations Manager, on 01962 848228

For more information or an application form please visit our website. Alternatively you can contact our Human Resources Team on, 01264 368106 or email jobs@testvalley.gov.uk

Closing date for return of application forms is Friday 8th June 2018.

COMMITTED TO EQUALITY OF OPPORTUNITY IN EMPLOYMENT AND SERVICES

Job Description & Person Specification

Job Title:	Senior Infrastructure Security Officer	Job Reference:	TBC
Service:	IT		
Location:	Beech Hurst, Andover, Winchester City Offices and other remote locations	Grade:	10
Reports to:	IT Operations Manager		
Date:	April 2018		

Our Values: We expect all of our employees to live by and demonstrate the Council's five key values of:

Accountability, Ambition, Empowerment, Integrity, Inclusiveness**.**

Main job purpose

To manage and maintain the ITIL Security Management Information System (SMIS) which protects all IT services including users, applications and hardware against cyber and security threats.

As part of the Operations Team, deliver a secure and operational IT Infrastructure to meet agreed performance indicators and service level agreements.

Project manage IT technical projects including security assessments of any new solutions.

Main responsibilities and duties

1. Provide IT Cyber Security expertise for the IT shared service across all functions including but not limited to:
   - The creation, maintenance and enforcement for all IT Security strategies and associated policy procedures.
   - Risk Management Assessments including financial impact and Council reputation damage limitation working closely with Audit teams and Third party support services.
   - Communicate effectively and adapt styles to the relevant audience which includes IT Management, IT Technical staff and end users. Host workshops and training sessions to improve Council staff and the IT team's security knowledge.
   - Work with the IT Service Desk and HR to induct new users on security. One to one sessions are required for GCSx users.
   - Assess all new IT solutions with weekly attendance and voting responsibility for the IT Change Advisory Board.
   - Consult with other security experts and professional bodies in relation to the latest security standards, threats and emerging trends.
   - Identify, analyse and manage the remediation of new threats and

vulnerabilities. This includes the creation of patch remediation scripts.
- Responsible for managing the response team as new threats are detected. You will be the central coordinator and maintain an up-to date status report as threats are time critical. You will be confident to make decisions on your own when required to safeguard the Council.
- Report to the IT Management team and senior Council managers on regular updates of any new threats and the risks associated with the threat to the Council. You will need to persuade and influence others to take the threat seriously.
- Maintain as part of a team the Infrastructure and application security with periodic health-checks and regular forensic testing. You will deliver daily security reports to the Operations Manager escalating any major risks.
- Manage compliance of all technical aspects of the Public Services Network (PSN) Code of Connection and the Payment Card Industry (PCI) data security standards.
- Respond to any official audit requests with a need for discretion and personal integrity to provide a professional service.

2. Work as part of the Operations team to:
   - Deliver 2nd/3rd line technical support and project work for Infrastructure solutions.
   - Project manage technical security projects and provide team leadership on other Infrastructure related projects reporting back weekly to the Operations Manager. These projects will range from 1-12 months in delivery.
   - Maintain complete and accurate technical documentation.
   - Resolve logged user calls as part of a team and identify improvements and trends to continually improve the service delivery. Working with users and other IT staff to ensure we meet Service Level Agreements and clearly communicate with minimal technical jargon on the resolution.
   - Participate in annual Business Continuity Plans and testing scenarios.

NB The particular duties and responsibilities attached to posts are of necessity in many cases somewhat difficult to define in detail, and may vary from time to time without changing the general character of the duties or the level of responsibility entailed.

Supervision and management

The role has no line management responsibility, but the post holder will be expected to act as a coach and mentor where appropriate.

Reports to the Operations Manager as part of the Service Delivery Team.

Resources

This post will use a Laptop and other IT mobile devices.

Contacts and relationships

This post holder will project manage IT staff.
They will influence staff to adopt new ways of working in line with changing security procedures.
They will support and train both IT staff and users at all levels to improve the workforce to detect and report security risks.

The will assist and provide written evidence to internal and external auditors and compliance officers. They will converse and challenge Third party IT solutions to identify any security risks and benefits from new and existing solutions.
Working environment
• This is an office based role with travel to remote sites. • There will be occasional lone working.

CRITERIA Everything included in this section needs to be able to be objectively measured in one of the following ways: application form, certificates, testing, interview or references.	**ESSENTIAL** **DESIRABLE**
Educational and professional qualifications	
• GCSE English Language and Maths or equivalent. • Educated to degree level or have evidence of relevant IT security experience. • Microsoft MCSA or similar in Windows 2012 Server and above. • Cisco CCNA or similar. • ITIL Foundation (v3) • CISM or equivalent security experience.	E E E D D D
Knowledge	
• Strong knowledge of security protocols. • Network, hardware and system architecture technical virtualisation, storage, LAN/WAN. • A thorough understanding of how to model security threats & risks as well as the controls necessary to mitigate them, on both an organisational and technical level. • Proven Cloud based computing.	E E E D
Experience	
• Demonstrable experience in the production of security compliance IT policies and procedures. • Experience of delivering PSN / PCI compliance and accreditation. • Proven experience of GDPR legislation, policies and techniques. • Experience of managing security in virtualisation / Cloud architecture and technology. • Proven experience in Microsoft Server, Active Directory domain management, Networking, LAN/WAN, storage. • Proven experience in delivering projects and 2nd/3rd level support. • Proven IT Call Management.	E E E E E E E

• Change Management. • IT System Audits.	E E
Key skills	
• Excellent written and verbal communication skills which can be tailored for a variety of audiences • The ability to work as part of a team to implement solutions and resolve incidents working to SLA's. • Ability to prioritise work, meet targets, follow procedures and work with minimal supervision • Able to make time critical decisions and justify with evidence reasoning for actions to protect the Councils IT Services and Data.	E E E E
Personal qualities and behaviours	
• Enthusiastic, proactive and confident. • A competent, flexible and supportive person who will be able to fit in with the team. • Flexible to work out of hours and take responsibility for their actions. • Able to work with minimum supervision and manage their own workload.	E E E E

Other Factors

- Participation in the out of hour's standby and call out rota may be required.
- Evening and weekend working may be required.
- Must be able to travel to Hampshire wide locations and occasionally to further locations some of which may not be easily accessible by public transport**.**

Corporate Responsibilities

All employees are required to adhere to corporate policies, procedures and codes of conduct; full details can be found on the intranet or from your line manager. Particular aspects include:

Health and Safety - Every employee while at work has a duty to take reasonable care for the health and safety of himself/herself and of other persons who may be affected by his/her acts or omissions at work - Health and Safety at Work Act 1974.

All employees are required to adhere to the Council's corporate policy, procedures associated with their duties and to undertake tasks/training in that context, as required.

Safeguarding - This Council is committed to safeguarding and promoting the welfare of children and young people and vulnerable adults and expects all employees and volunteers to share this commitment, and to adhere to the Council's Safeguarding Policy.

Equalities – This Council is committed to providing equal opportunities for all. We believe that employing people from different backgrounds with a range of perspectives and experiences helps us to deliver high quality services to all our residents. We employ people based on their abilities and potential, regardless of any

protected characteristics.

Social Media - Employees are required to adhere to social media corporate policies and to undertake tasks/training in that context as required. Employees must not bring the Council into disrepute through their use of social media either personally or on behalf of the Council.

Financial – Employees are required to adhere to the Council's financial regulations and to undertake tasks/training in that context, as required.

Risk Management - Employees are required to adhere to the Council's risk management strategy and to undertake tasks/training in that context, as required.

Data Protection and Data Security - We hold and process information about our customers and as such we are legally obliged to protect that information.
Data protection is important for the Council, and employees are required to understand and adhere to relevant policies and procedures.