

## Job Description

|                   |                                 |
|-------------------|---------------------------------|
| Service:          | 3C ICT Shared Services          |
| Job title:        | Cyber/Information Security Lead |
| Grade:            | H                               |
| Hours of work:    | 37                              |
| Responsible to:   | Deputy Head of ICT & Digital    |
| Responsible for   |                                 |
| Direct reports:   | Information Security Officer(s) |
| Indirect reports: | 0                               |
| Budget:           | None                            |

### Purpose of Post:

The Cyber/Information Security Lead role will be responsible for maintaining the Confidentiality, Integrity and Availability of the 3C Shared Service IT Infrastructure.

The role assumes responsibility for monitoring and checking all facets of computer security. This will involve planning and implementing security measures to protect a business's data and information from deliberate attack, unauthorized access, corruption, and theft.

Working with the Technical Architect, you will ensure resilience, IT Security, Data Protection, Best Practice and Information Governance requirements are in line with the UK Governments Cyber Security Strategy adopting a 'Secure by Design' stance.

### **Key Deliverables:**

- Responsible for providing information security expertise to all 3C ICT shared service staff and partners.
- To ensure that the IT support service is customer focussed, efficient, effective and delivered to the highest possible standards.
- Develop, implement and review all IT Security policies.
- To ensure that the appropriate security controls are applied to all systems.
- To ensure the highest possible standards of IT Security are included in all operating processes including incident, change and problem management.
- Working with the Technical Architect and stakeholders to ensure the smooth implementation and integration of new systems and infrastructure using the 'Secure by Design' method.
- Continuous monitoring of all IT systems and detailed report analysis for breaches and threats.
- Attend Information Governance meetings including provisions and presentation of a cyber security report.
- Represent 3C ICT at public sector partnerships to understand partner threats as well as representing 3C ICT's posture. Including but not limited to attending WARP or CyberUK.

### **Main duties and responsibilities:**


- Evaluate the weak points and risks to computer systems creating plans to reduce possible threats.
- Forensic investigation and liaising with the Information Governance Manager and relevant bodies for any cyber breaches.
- Developing IT disaster recovery plans ensuring restorative actions in the event of a cyber security breach.
- Conduct formal training seminars on the use of the systems and products.
- Identify and interpret customer requirements, risks, and issues, giving a range of evaluated options and solutions.
- Provide a structured approach to diagnosing, assimilating and critically interpreting project objectives, risks, and issues.
- Analyse and design processes to ensure that specifications/guidance continue to meet the needs of users.
- Lead development activities for allocated work packages. Plan, schedule, co-ordinate, monitor and adjust the resources (human and physical), activities and priorities in order to deliver work packages to agreed objectives, standards and deadlines.
- Develop and maintain an understanding of 3C Shared Service policies and strategy. Assess the impact of these policies and strategies across the stakeholders IT systems and services assisting in the development of proposals for change where appropriate.

- The production of report and compliance data from Cyber Security Systems and monitoring of the 3C Shared Service digital estate to ensure systems are patched and protected against known and emergent threats.
- To ensure that all assets and associated configurations for services are registered and managed.
- Work with auditors to ensure Cyber Security Systems are compliant with external assessors.
- Some work is clearly defined by expected results, but much functional requirement will need to be established through interpretation of broad occupational policies.

|  |   |
|--|---|
| <p><b>Knowledge and Qualifications</b></p> <p>The minimum knowledge required to undertake this role and any qualifications or training essential for the role</p> <p>(E) Essential<br/>(D) Desirable</p> | <p>(E) Essential</p> <ul style="list-style-type: none"> <li>• A strong commercial understanding of Information/IT Security.</li> <li>• Network Security/Data Security knowledge.</li> <li>• Strong understanding of ISO 27001/Cyber Essentials Plus/other applicable accreditation.</li> <li>• Knowledge of cyber security risks and mitigation.</li> <li>• Vulnerability and penetration testing using industry standard tools.</li> <li>• Excellent knowledge of security best practices.</li> <li>• Educated to degree level or equivalent experience and a recognised qualification. i.e. CISSP, CISM, Security + or similar certifications.</li> <li>• Industry standard IT qualifications e.g. Microsoft, Cisco, ITIL.</li> </ul> |
| <p><b>Experience</b></p> <p>Experience the person would need to do the job</p> <p>(E) Essential<br/>(D) Desirable</p>  | <p>(E) Essential</p> <ul style="list-style-type: none"> <li>• Recent experience in a Cyber Security role.</li> <li>• Good working knowledge of IT Security best practice.</li> <li>• Excellent knowledge of proactive risk management.</li> <li>• Effective communication of IT Security principles to all levels of the organisation.</li> <li>• Experience of ITIL-based Change Control and CMDB would be beneficial.</li> <li>• A good Technical understanding of application and network security.</li> <li>• Experience in providing relevant technical/security support at appropriate level.</li> <li>• Working with SIEM solutions.</li> </ul>  |

|  |   |
|--|---|
| <p><b>Skills and Abilities</b></p> <p>Specific skills the applicant would need to do the job</p> <p>(E) Essential</p> <p>(D) Desirable</p> | <ul style="list-style-type: none"> <li>• A working Knowledge of Health Computing Systems or a similar SME and data structures.</li> <li>• Experience with network and switch technologies such as WiFi, VLANs, Routers, Switches, Firewalls etc.</li> <li>• DHCP, DNS, Active Directory, Group Policy, and Exchange.</li> <li>• Mobile Device management.</li> <li>• Virtual Server Management (VM Ware).</li> <li>• Ability to maintain confidentiality of personal information.</li> <li>• Ability to communicate complex information to individuals or to groups of people.</li> <li>• Analytical and logical approach to problem solving.</li> <li>• Root Cause Analysis of security incidents.</li> <li>• Experience of working with minimum supervision, with the ability to use initiative and experience to present solutions to overcome technically challenging issues.</li> <li>• Experience of Penetration and Vulnerability Testing tools and techniques.</li> <li>• Able to evaluate and assist in selection of best practice security tools.</li> <li>• Use of Service Desk Tools and Technologies.</li> <li>• Proficient in Microsoft Desktop operating systems and applications.</li> <li>• Understanding of Information Security principles.</li> <li>• Knowledge of the Data Protection Act.</li> <li>• PowerShell scripting.</li> </ul> |
| <p><b>Decision Making and Impact on Others</b></p>   | <p><b>Innovation</b></p> <ul style="list-style-type: none"> <li>• Challenges the status quo: suggests new approaches to old problems</li> </ul>   |

|  |   |
|--|---|
| <p>What impact the reasons made by the post holder would have on others across the Council</p>   | <ul style="list-style-type: none"> <li>• Promotes and demonstrates continual improvement</li> <li>• Generates new ideas and creative solutions</li> <li>• Applies existing methods in new ways or new situations</li> <li>• Seeks new ideas.</li> <li>• Shares innovative practice with others</li> </ul> <p><b>Decision Making</b></p> <ul style="list-style-type: none"> <li>• Makes and communicates clear decisions</li> <li>• Makes effective decisions under time pressure</li> <li>• Balances risks and benefits of various options and decisions</li> <li>• Takes responsibility for the outcomes and impact of their decisions and those they delegate</li> <li>• Considers all relevant data when making decisions</li> </ul> |
| <p><b>Communication with Internal and External Customers</b></p> <p>What customers the applicant would be in contact with in the job</p> | <ul style="list-style-type: none"> <li>• Ability to interpret and communicate complex technical information to both technical and non-technical staff.</li> <li>• Ability to communicate effectively to both internal and partner staff at all levels throughout the organisations.</li> <li>• Requires excellent communication skills both verbal and written and have the ability to communicate effectively, both formally and informally to all levels of staff.</li> <li>• Provide clear reports to senior management.</li> </ul> <p>Internal customer contact 60%</p> <p>External customer contact 40%</p>  |
| <p><b>Personal Attributes and Other Requirements</b></p>   | <ul style="list-style-type: none"> <li>• Ability to remain calm and composed in high pressure situations.</li> </ul>  |

|   |  |
|---|--|
| <p>In this section please list any other qualities you are looking for from the applicant</p> <p>(E) Essential</p> <p>(D) Desirable</p> | <ul style="list-style-type: none"> <li>• Self-motivated and able to work to tight deadlines with a flexible approach to work.</li> <li>• Able to form good working relationships with staff across the partnership and partner organisations.</li> <li>• Willing to develop own skills and knowledge.</li> <li>• Ability to work as a member of a team.</li> <li>• Excellent inter-personal skills.</li> <li>• Ability to work in a busy environment where continuous interruptions and re-prioritisation of workload is to be expected.</li> <li>• Ability to lead and motivate a team.</li> </ul>  |
| <p><b>HDC values</b></p>                             | <p>The values outlined below reflect our collective positive attitude and how all staff are expected to work together as one team.</p> <p><b>Inspiring:</b> We have genuine pride and passion for public service; doing the best we can for customers matters to us all.</p> <p><b>Collaborative:</b> We achieve much more by working together, and this allows us to provide the best service for customers.</p> <p><b>Accountable:</b> We take personal responsibility for our work and our decisions, and we deliver on our commitments to customers.</p> <p><b>Respectful:</b> We respect people's differences and are considerate to their needs.</p> <p><b>Enterprising:</b> We use drive and energy to challenge the norm and adapt to changing circumstances. We are always ready for challenges and opportunities, and we embrace them.</p> |

**Safeguarding and promoting the welfare of children and young people/  
vulnerable adults**

Huntingdonshire District Council is committed to safeguarding and promoting the welfare of children and vulnerable adults and expects all staff and volunteers to share this commitment.

- Can demonstrate an ability to contribute towards a safe environment
- Is up-to-date with legislation and current events
- Can demonstrate how s/he has promoted 'best practice'