

SOUTH WALES FIRE AND RESCUE SERVICE
JOB DESCRIPTION

| | |
|---|--|
| Department | Information Communications Technology |
| Post | ICT Security Specialist |
| Post No | 505645 |
| Grade | Grade 12 (£38,223 - £39,186) |
| Location | South Wales Fire & Rescue Service Headquarters |
| Responsible to | ICT Service Manager |
| Responsible for | Virtual Security Team |
| Responsibility for Physical Resources | ICT Equipment |
| Responsibility for Financial Resources | ICT Delegated Budgets (Revenue and Capital) ICT Project Budgets |

This job description refers to the main purpose and responsibilities of the post. It does not necessarily list in detail all of the tasks required to carry out these responsibilities. This job description will be reviewed as and when necessary to ensure that it meets the Service's business requirements.

MAIN PURPOSE OF THE POST

To effectively plan and manage all Cyber security functions of the South Wales Fire & Rescue Service.

Develop and Train the Virtual Cyber Security ICT team and wider organisational staff to create effective Cyber risk prevention, incident detection and response capabilities.

DUTIES AND RESPONSIBILITIES

1. To provide Strategic Management and technical leadership identifying development opportunities. Planning, implementing change and Integration across teams, and necessary business processes to develop an effective Cyber Security culture and response capability.
2. Responsibility for security project management including project budgets through the complete project lifecycle. Undertaking proactive monitoring of costs, timescales and ensuring ICT resources are planned, scheduled, appropriately assessed for risks and impact in order to meet relevant project delivery deadlines, whilst maintaining a focus on service delivery.
3. Responsible for the planning and implementation of security policies, procedures and processes, to ensure secure system provisioning and

Date May 2024

Author: Chris Williams – Head of ICT

maintenance that is consistent with industry best practices, regulatory requirements and the ICT Strategy to ensure that a high-quality service is provided and maintained.

4. Undertake Critical Incident Team (CIT) functions as directed in relation to the Organisations and Local Resilience Forums (LRF) Disaster Recovery Plans (DRP) including assisting developing such plans.
5. Responsibility for any needed service accreditation against National and Welsh Government Security policies and guidance, including that from the NFCC, NCSC and CPNI e.g. Cyber Assessment Framework (CAF), Cyber Essentials, Information Assurance of Small and Medium Enterprises (IASME), ESN (Emergency Services Network), Airwave CoCo (Code of Connection) and to undertake and act on the findings of any IT Health Checks needed to achieve those.
6. To track sources of intelligence including open and 'FRS only' available to ensure an up to date and timely management of emerging risks. E.g. through active membership in NCSC ACD, Cymru WARP, NFCC Cyber Group, CiSP, Cymru SOC and Microsoft M365 Threat Intelligence.
7. To co-ordinate security project work packages to other Team Managers.
8. Responsible for the design, implementation, operation and maintenance of the Information Security Management System.
9. To coordinate the development of the ICT Business Continuity Plans in relation to Cyber Security.
10. Responsibility for the management of existing ICT related security related contracts and tenders.
11. To create technical specifications and functional requirements for internal and externally contracted works and subsequent support.
12. Develop and promote an enhanced reporting structure to the corporate Security Risk Group which ensures the early identification of issues and ensures minimum risk to the business continuity of the organisation.
13. To provide Support and Guidance on all ICT Security related problems and requests for advice relating to the usage and implementation of available / proposed systems.
14. Work closely with decision makers within the organisation and with collaborative partners in order to identify, recommend, develop, implement, and support cost-effective security solutions.
15. Represent ICT and the service as a subject matter expert at internal i.e. Security Risk Group (SRG), external and national groups when required

16. To provide security assessments and to ensure that adequate provision is made to secure information systems and data from loss using appropriate risk management methods.
17. To promote and ensure physical and data security of the service systems are maintained and monitored to deter and prevent Cyber-attack. To develop appropriate response plans to deal with such incidents.
18. To audit and ensure accurate records are kept of all user accounts to include access and security, location and group management.
19. Responsibility to monitor, audit and ensure Incident, Problem, Change and Release Management functions are effectively carried out to maintain and improve service quality for Security Systems:
 - ICT Incident Management, responsibility to oversee restoration of normal operations as quickly, with the least possible impact on either the business continuity or the user, and efficiently as possible with regard to resource and cost.
 - ICT Change Management, responsibility to ensure standardised methods and procedures are used for efficient and prompt handling of all changes to the ICT environment, in order to minimise the impact of change related incidents upon service quality, and consequently to improve the day-to-day operations of the organisation in relation to Service Provision and Business Continuity
 - ICT Release Management, oversee and audit configuration items within the organisation, their management, deployment, support and licensing.
20. Provide 3rd line support in the provision of complex incident and problem resolution. To provide all relevant technical expertise required for service support.
21. To audit the receipt and payment of goods within the ICT Budget where appropriate.
22. To ensure the correct disposal of redundant equipment within the Waste Electrical and Electronic Directive and Hazardous Waste Regulations.
23. Responsible for the adherence to and promotion of practices and activities associated with all Service policy and procedures including Health and Safety, Diversity and Equal Opportunities.

The Service is committed to promoting the use of Welsh Language in all aspects of the business.

STANDARD SERVICE REQUIREMENTS

Date May 2024

Author: Chris Williams – Head of ICT

- To attend in-house and external training courses as required.
- Any other duties commensurate with the grade and post.
- To co-operate fully with any scheme or pilot scheme that shall be introduced within the department or across the Service.
- To implement the principles of the Service's Equal Opportunities and Diversity Policies and Welsh Language Schemes whilst carrying out the above duties.
- To adhere to Health & Safety Legislation/Relevant Service Policies and Procedures and to take reasonable care for the health and safety of yourself and other persons who may be adversely affected by your acts/omissions.

ORGANISATIONAL VALUES

In performing the above role, all employees of the Service are required to observe and promote the Service's Core Values to be, at all times:

- Professional
- Caring
- Respectful
- Dedicated
- Trustworthy
- Dynamic
- Disciplined
- Resilient

