



Gwasanaeth Tân ac Achub
Canolbarth a Gorllewin Cymru

Mid and West Wales
Fire and Rescue Service

JOB APPLICATION PACK

www.mawwfire.gov.uk



Introduction

Dear Applicant,

Thank you for your interest in joining Mid and West Wales Fire and Rescue Service.

My vision is for our Service 'to be a world leader in emergency response and community safety.' Whilst we have a proud track record of achievement, we know that there is always room for improvement.

When people think of a career in the Fire and Rescue Service, they tend to think of Firefighters responding to emergency incidents, but it's not just Firefighters who make mid and west Wales a safer place.

Behind the operational scene, the Service has a large range of other posts within different departments which are either office based or in our workshops, and we employ people in professional, technical, and administrative roles.

Without corporate support functions in place to provide the systems, processes and technology, the Service would not be able to deliver the best possible service to our communities.

If you're looking for a career with variety, a challenge, and opportunities for progression, along with all the benefits you'd expect from a key public service organisation, then why not consider joining us in one of our specialist or administrative support functions.

Thank you and good luck



Roger Thomas
Chief Fire Officer, Head of Paid Service



Our Vision:

**To be a World Leader in
Emergency Response and
Community Safety**

Our Mission:

**To Engage, Connect,
Develop and Inspire people
to deliver an excellent
Service**

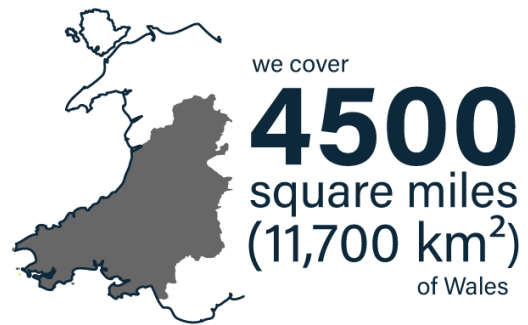
Our Values:

- **Do the Right Thing**
- **Treat People with Respect**
- **Perform with Excellence**





About the Service



The Service was created in 1996 by the Local Government (Wales) Act 1994, following the merger of Dyfed, Powys and West Glamorgan Fire Brigades. Mid and West Wales Fire and Rescue Service covers the following County Council areas:

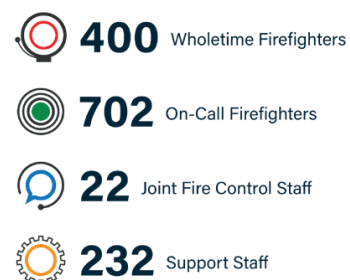


The Service makes up almost two-thirds of Wales, covering a predominantly rural area of 11,700 km² (4,500 square miles), with 650km of coastline. With its Headquarters in Carmarthen, the Service employs 1300 staff, with a little over a 1100 of those based in one of 58 stations spread across three Divisions. The Service has the third highest population sparsity in England and Wales and there are 900,000 people that live within our Service area. This number increases to over 2 million as a result of tourism through the summer months.

It is the third geographically largest Fire and Rescue Service in the United Kingdom, behind the Scottish and Northern Ireland Fire and Rescue Services. This in itself presents a range of different challenges.

There are a variety of risks found within the Service area, ranging from the petrochemical industries in Milford Haven, to the risks associated with heavily populated areas such as Swansea and Neath Port Talbot. There is also a large farming community and many other light industries throughout the area.

These, together with an extensive coastline and inland waterways, form some of the specialised risks found within the Service.





Benefits

Working for the Service opens the door to a whole portfolio of benefits which can enhance your lifestyle both now and into the future.



Competitive rates of pay -
recently reviewed to ensure fairness across all roles; with annual increments to the top of your salary band, as you build knowledge and experience.



Local Government Pension scheme -
A generous pension scheme, with the Service making a substantial contribution (currently 15.1%) to funding your retirement, as well as the option to increase your benefits by purchasing additional pension or investing in Additional Voluntary Contributions (AVC).



Generous Annual leave -
26 Days plus bank holidays, going up to 33 days after 5 years employment.



Flexi Scheme -
Opportunity to flex your working hours to help accommodate life outside of work.



Free on-site parking



Cycle to Work



Staff Discount scheme



Health and Wellbeing

- Access to Blue Light Card discount scheme
- Car Leasing Salary Sacrifice scheme
- Let's Connect IT equipment loan scheme
- Subsidised canteen facilities
- Sports and Social Club
- Firefighters Charity



A Work Environment Shaped by our Values

Committed to Equality and Diversity -

Equality, diversity and inclusion is at the heart of what we do as a Service and are values which sit at the core of our organisational processes, practices and culture.

As a service, we are committed to identifying, understanding, and eliminating all barriers that prevent access to services, information, and employment.

The Service currently has a small number of internal employee networks / forums in place, which play an active role in:

- Championing issues for employees;
- Contributing to the organisation's diversity and inclusion agenda;
- Advising on policy development;
- Improving the work environment for employees



Committed to reducing our Environmental Impact -

We recognise that our operations have an effect on the global and local environment and are committed to minimising adverse environmental impacts within financial, operational and resource constraints.

In our race to Net Zero Carbon Status by 2030, the Service has set itself targets that align with the Welsh Government route map for decarbonisation across the Welsh public sector.

The Service has achieved Level 5 Green Dragon Environmental Standard accreditation for the 8th year in a row.

#CARBONZERO30



Job Profile

Salary:.....£34,834 – 36,648.....

About this Job

This is a great role for someone who loves the Cyber Security challenge, being the protector of our Service Network, Systems and Data and ensuring the best security principles are applied.

It will require someone who has great integrity, super attention to detail, adaptable to new challenges, a thirst for new learning and continuous improvement and can keep calm under pressure.

Mid and West Wales Fire and Rescue Service is committed to providing the highest level of service to our community. We are looking for a dedicated ICT Cyber-Security Officer to join our team and help us maintain our cyber-resilience. The role is part of the ICT department based at our Carmarthen HQ, but we have option for some agile working from an alternative location. We have parking, electric car chargers and a staff canteen onsite.

As an ICT Cyber-Security Officer, you will be responsible for real-time monitoring and auditing of system and network security events. You will work closely with, and report to, the ICT Security and Compliance Manager to promote a positive cyber security culture across the organisation.

Key Responsibilities:

- Monitor alerts from a range of systems and providers, triage and prioritise the results and take action against any threats.
- Ensure any security recommendations are assessed and changes added to the Change Advisory Board for approval.
- Manage our SIEM and network monitoring systems to spot issues or indicators of compromise.
- Ensure systems are configured with best practice security principles.
- Analyse new threats and vulnerabilities and ensure they are mitigated.
- Provide advice on new systems to ensure they are configured securely.
- Promote security awareness and help with security training across the Service.

This role needs someone with in-depth knowledge of modern cybersecurity and cyber resilience either through current experience in the field or rigorous high-level training, such as a degree in the subject, or a combination of the both.

Experience or good practical knowledge of SIEMS, Microsoft Security tools, IDS or similar is required.

Interested? Apply now and become a part of our dedicated team!



Job Description

TITLE OF POST:	ICT Cyber-Security Officer
RANK/ROLE:	Grade 8
POST REFERENCE:	
LOCATION:	ICT Department, Service Head Quarters, Carmarthenshire
RESPONSIBLE TO:	ICT Security and Compliance Manager
MAIN PURPOSE OF JOB:	Provide real-time monitoring and auditing of system and network security events to ensure the Services Cyber-resilience is maintained. Working with the SICT Security Manager to proactively ensure a positive cyber security culture across the organisation.



SCHEDULE OF RESPONSIBILITIES

RESPONSIBLE TO

1. Assist with keeping the ISPD up to date and relevant for our organisation	Team Manager
2. Assist with ensuring that the Business Continuity plans are up to date and relevant to ICT and our organisation and assist with business continuity exercises.	Team Manager
3. Ensure that systems are configured with best practice security principles, including up to date patching, software updating and/or mitigations are in place.	Team Manager
4. Ensuring all new threats and vulnerabilities are analysed to see the impact to the Service, categorised and then passed to the responsible team to ensure they are fixed or mitigated with an appropriate deadline	Team Manager
5. Suggest security implications with a risk assessment to the Security team manager and/or the Head of ICT	Team Manager
6. Work with the Data Protection Officer to ensure that Data Protection principles are followed and adhered to	Team Manager
7. Ensure that disaster recovery systems, including backups, are working and tested	Team Manager
8. Provide advice on new systems that are being brought into service to ensure they are configured securely	Team Manager
9. Advise on creating secure images for ICT hardware and other security enhancements that would be beneficial and are risk assessed.	Team Manager
10. Provide monitoring, evaluation and configuring of Malware, Phishing, quarantining features etc on the e-mail system	Team Manager



11. Help to ensure compliance with software licensing requirements	Team Manager
12. Ensure that compliance and legislation is followed across the department and ICT specific procedures are followed across the Service area.	Team Manager
13. Promote security awareness and help with security training across the Service in conjunction with the Security Team manager and the ICT Training Officer	Team Manager
14. Keep abreast of best practice for ICT security especially within the Fire Service	Team Manager
15. Assist with providing information required for Freedom of Information requests	Team Manager
16. Seek out and sign-up to regular security bulletins from trusted sources, vendors, sector partners and reputable news sources including relevant CVE reports and review these bulletins in a timely manner.	Team Manager
17. Root cause analysis of any identified security incidents, with a written report and lessons learnt as directed by the team manager.	Team Manager
18. Proactive searching for security issues, indicators of compromise, privileged access and risky user logs within all ICT systems and infrastructure	Team Manager
19. Detection and understanding of system abnormalities across the Organisation	Team Manager
20. Monitoring, in real-time, logs, alerts, system issues and user related security events using all the tools available to you to detect intrusions, threats and data loss prevention to our network, systems and data. Reporting adverse finding to your team manager.	Team Manager



21. Ensure security monitoring systems and AV is working correctly and updating regularly across all devices in the organisation	Team Manager
22. Keeping the authorised software list up to date, ensuring the configuration is in place, adding exceptions to trusted software and Attack Surface Reduction rules as required	Team Manager
23. Generating regular security reports in a language that can be understood by all members of the organisation.	Team Manager
24. Performing regular vulnerability scanning and pen testing to find potential issues or rogue hardware or software.	Team Manager
25. Ensure that all changes are put into the ICT Change management process and ICT risks are recorded on the ICT risk register.	Team Manager
26. Advising staff when they report security related issues and reacting to any confirmed threats.	Team Manager
27. Working with third party security providers as required.	Team Manager
28. Testing and deployment of new security policies.	Team Manager
29. Regularly review security policies, staff privileges, guest access and other related configurations (at least six monthly)	Team Manager



General Responsibilities

1. Help to ensure that the SLA for department is monitored and adhered to where practical for your role	Team Manager
2. To attend technical training and system familiarisation courses as and when required (including with required overnight stays)	Team Manager
3. Represent the ICT department in meetings, working groups and similar as required by your team leader or Head of ICT	Team Manager
4. Ensure all areas of the office, workshop and storage areas are kept clean and tidy, all stock is correctly labelled and, where appropriate, disposed of quickly through service policies.	Team Manager
5. Ensure staff are compliant with the ISPD and that all work carried out is done with respect to the policy and other Service policies such as Data Processing policies..	Head of ICT
6. To comply with health and safety guidelines and all other Service employment related policies	Head of ICT
7. To undertake any other duties as directed by your line manager or Head of ICT commensurate with wider departmental responsibilities	Team Manager/Head of ICT
8. Ensure any ICT requests for support are logged to the ICT helpdesk.	Team Manager
9. To help develop, disseminate and promote IT related good practices throughout the organisation including those relating to software security and licensing	Team Manager
10. Have a full driving licence. Be able to drive at all times in a safe and secure manner.	Head of ICT



11. Helping to ensure the current Service objectives are delivered and reported on	Head of ICT
12. Help with any Audits of the department, systems or Software as required.	Head of ICT
13. Ensure that all procurement is carried out in a manner that follows the Service procurement policy.	Head of ICT
14. Complete regular self-directed learning as required for your role or as directed by the Head of Department to ensure you have continuous personal development	Head of ICT



Gwasanaeth Tân ac Achub
Canolbarth a Gorllewin Cymru
Mid and West Wales
Fire and Rescue Service

MID AND WEST WALES FIRE AND RESCUE SERVICE

PERSON SPECIFICATION

POST TITLE	ICT Cyber-Security Officer
LOCATION	Service Headquarters, Carmarthen
POST NUMBER	
GRADE	Grade 8
DEPARTMENT	I.C.T. Department
DBS CHECK	Standard

Please ensure you address each of the following requirements in your Application Form as they will be used for shortlisting purposes. You should provide clear evidence that demonstrates you meet each area based on your skills, knowledge, experience and abilities relevant to the post.

Factor	Evidence	Essential/ Desirable	Assessment Method
Qualifications	Industry recognised cyber-security qualification such as cyber-security degree, or a combination of CEH, CCSP, CISMP, CCP Scheme or equivalent that provides a high degree of technical, real-world understanding of Cyber-Security and Cyber-resilience. AND/OR Working in a cyber-security role with at least 3 years experience in an organisation with a very strong cyber-security culture and working to industry best-practices. Other ICT industry recognised qualifications in Systems, Networks, firewalls etc Microsoft 365, Cloud administration or similar qualifications. Full Driving Licence Pen-testing or Ethical Hacking courses	Essential* Desirable Desirable Essential* Desirable	Application form and Certificates



Knowledge			Application form and Interview
	Good understanding of technical terms, ICT hardware and software, contemporary ICT best practices.	Desirable	
	Good knowledge of intrusion detection systems and indicators of compromise	Essential*	
	Understanding of MITRE attack or Cyber Kill Chain techniques and mitigations	Desirable	
	Current cyber-threats to organisations	Essential*	
	Knowledge of incident management processes and playbooks	Essential*	
	Great knowledge of cyber-security, including best practices, effective secure configurations, contemporary security risks and aligning to secure frameworks or standards.	Essential*	
	Understanding and evaluating risk in a cyber-security context	Essential*	
	Working within public sector procurement and governance frameworks.	Desirable	
	Knowledge of ICT Change Management	Desirable	
	Good knowledge of device hardening in an ICT security context	Desirable	
	Awareness of ISO 270001, Cyber-essentials, Cyber Assessment Framework and working to those standards.	Desirable	
	Good understanding of business continuity, disaster recovery and incident management	Desirable	
	Knowledge of NCSS best practice, guidance and available tools	Desirable	
	Good understanding of effective product or solution research	Desirable	
	Good knowledge of using, analysing and interpreting Microsoft Security Suite products and its security recommendations.	Desirable	



Experience	<p>Working within the Public Sector</p> <p>Working in ICT within the Emergency or Security Services</p> <p>At least 3 years configuring systems and networks to defend against cyber attacks and ensure cyber resilience</p> <p>Analysing log, alerts, vulnerabilities and security recommendations, risk assessing them and providing guidance on mitigation</p> <p>Ability to evaluate value for money effectively</p> <p>Working hands-on with configuration of Microsoft systems, including Microsoft 365 Administration, Virtual Machine configuration, SANs, Firewalls and network infrastructure</p>	<p>Desirable</p> <p>Desirable</p> <p>Desirable</p> <p>Essential*</p> <p>Desirable</p> <p>Desirable</p>	Application form and Interview
Job Related / Personal Skills	<p>Ability to work under pressure</p> <p>Ability to use own initiative and proactively seek out information</p> <p>Ability to work as part of a team</p> <p>Ability to triage and manage different priorities effectively</p> <p>Enthusiastic and committed approach to providing a quality service</p> <p>Ability to manage time effectively as well as estimating time and resources required accurately</p> <p>Analytical thinking skills</p>	<p>Essential*</p> <p>Essential*</p> <p>Essential*</p> <p>Essential*</p> <p>Essential*</p> <p>Essential*</p> <p>Essential*</p>	Application form and Interview
Communication	<p>English verbal and written skills</p> <p>Welsh verbal and written skills (Level 1 – Basic Greetings)</p> <p>Welsh verbal and written skills (Level 2+)</p> <p>Ability to communicate technical subjects well and with accuracy</p> <p>Working effectively with external suppliers of products and services</p> <p>Ability to create easy to understand and engaging reports and technical documentation</p>	<p>Essential*</p> <p>Essential*</p> <p>Desirable</p> <p>Essential*</p> <p>Desirable</p> <p>Essential*</p>	Application form and Interview



In line with the Service's Recruitment and Selection procedure, a standard disclosure is required as a minimum for all roles.

Certain roles will be subject to increased levels of DBS check, dependent on the duties and responsibilities of the role, and as designated by the relevant Head of Command or Department.

Where a requirement for a higher level of DBS check has been identified the level and justification for this is specified below:

LEVEL: Standard

JUSTIFICATION:

PREPARED BY: **Head of ICT**

DATE REVIEWED: **May 2024**



How to Apply

Closing Date:

The information provided on the application form is key information that will be used in the short-listing process. It is therefore important that the guidance notes below are followed when completing the application form. This will ensure all the relevant information is available to make a decision on whether you will be short listed for interview. Short listing will involve assessment of the details provided on the application form against the criteria outlined in the Person Specification provided.

Applications will be accepted in other formats where an applicant has difficulty completing the standard form as a result of disability.

What happens after you've sent in your application?

Once we've received your application, we will separate the equal opportunities monitoring form which will not form part of the selection process and will send the application form only to the shortlisting department. We will send an acknowledgement of receipt to all applicants.

Your application will then be assessed against the criteria (in a person specification) and the shortlisting panel will decide whether it can be shortlisted.

If you are not shortlisted for interview, you will be advised in writing, usually within six weeks of the closing date. If you have not heard from us by then, please contact us.

If you are shortlisted for interview, you will receive an email from us usually within 2-3 weeks of the closing date, advising the date, time and location of the interview. The email will also include details of assessment testing which is to be carried out and will contain the documentation which you are required to bring with you, if applicable to the role.



Gwasanaeth Tân ac Achub
Canolbarth a Gorllewin Cymru

Mid and West Wales
Fire and Rescue Service

www.mawwfire.gov.uk