UK Parliament Digital Service

Supporting a thriving Parliamentary democracy

Job Description

Job Title:	**Identity and Access Management Lead**
Directorate:	Platforms
Banding:	A2
Reporting To:	Identity and Access Management Service Owner

The Role

As the Identity and Access Management Lead, you will act as the technical subject matter expert and lead on defining and delivering a vision for the Identity and Access Management product / service. You will be responsible for owning, maintaining and evolving innovative technology products and services that deliver maximum value for users with a strong commitment to continuous improvement.

You collaborate with the Identity and Access Management service Owner and colleagues across the Digital Service and beyond to provide a highly available, secure and reliable Identity and Access Management service

Key Responsibilities

- Maintains standards of excellence across all areas of delivery, including user experience, accessibility, reliability, performance and delivering a high-quality service.
- Day-to-day management of the product service backlog: actively limiting work in progress, removing blockers and prioritising the flow of work to ensure that the user need is paramount in all delivery. Proactively monitors and reviews the performance of the Identity and Access Management product service, managing availability, capacity and acting as the key point of contact during major incidents.
- Promotes and optimises the use of monitoring and analytics tools for performance and uptake metrics for the product and service. Develops and implements automated processes, wherever possible, for the control and early warning or prediction of issues.
- Collaborates with the Identity and Access Management Service Owner to input into architecture, roadmap and standards for Identity and Access Management.
- Provides technical direction and advice to programmes and projects. Recognises, and actively seeks ways to exploit technology to address complex business, organisational and technical issues, of both a conventional and innovative nature.
- Proactively manages the ongoing support model for new technologies, ensuring that service design is built into proposals from the outset.

- Provides input into business cases as appropriate, promoting innovative solutions and design options, which deliver maximum value for users. Inputs into operational plans, policies, procedures and transition/migration plans.
- Ensures a culture of open and inclusive collaboration across the team. Actively supports and encourages the creation of multi-skilled technical teams within a product-centric environment.
- Proactively encourages diversity and inclusivity taking practical steps to improve and maintain workforce diversity, ensuring effective succession planning and skills development.
- Identifies, owns and mitigates risks associated with the X product and service, ensuring cyber security is considered and embedded into every aspect of how X operates including compliance with all agreed UK Parliament policies

The above list of key responsibilities is not exclusive or exhaustive and the post holder will be required to undertake such tasks as may reasonably be expected within the scope and banding of the post.

About Us

The Parliamentary Digital Service, a joint department of both Houses of Parliament, provides technology and intranet services to all Parliamentary users. It is also responsible for the strategic direction of Parliament's digital offering through Parliament's Digital Strategy and the delivery and management of parliamentary digital platforms, including the website. We support Parliament through our team of over 450 dedicated and professional digital colleagues.

Our Values

The post holder will be expected to operate in line with the Parliamentary Digital Service workplace values which are:

Care – Caring for ourselves, each other, and the people who use our services

Confidence – Believing in the value of what we do and showing pride in our work

Community – Working together as one team and building communities to share skills and expertise

Curiosity – Learning, listening, and challenging to be the best at what we do

The Requirements

Criterion 1

Experience in successfully designing, implementing and supporting Identity and Access Management solutions, with specific knowledge and experience of: PKI infrastructure and certificate management, Utilising HSMs, Azure Active Directory including features such as PIM and Conditional Access, ADFS Management / Azure MF Authentication /AAD Connect, Securing of Active Directory both on-premises and Cloud, Azure B2B & B2C.

Criterion 2

Outstanding planning and organisational skills to work within tight deadlines, cope with fluctuations in workload and deliver results within agreed timescales.

Criterion 3

Experience of defining and reporting progress against targets, providing highlights as necessary and taking actions to resolve exceptions.

Criterion 4

Excellent written and verbal communication skills with the ability to present complex information clearly and effectively whilst upholding the values of equality, diversity and inclusion.

Criterion 5

Strong sense of customer service and demonstrates an understanding of the needs of customers, keeping them in mind when taking actions or making decisions.

Criterion 6 *(desirable)*

A good awareness and understanding of the following would be beneficial: Windows OS, Microsoft Identity Manager, One Identity (active roles). Remote Access technologies (such as DirectAccess and Cisco VPN) and PowerShell Scripting.