UNIVERSITY OF LEEDS

CANDIDATE BRIEF
Identity and Access Management Lead, IT

Salary: Grade 9 (£51,799 - £60,022)

Reporting to: Chief Information Security Officer (CISO)

We will consider flexible working arrangements

Overview of the Role

We are looking for an Identity and Access Management Lead to join our Cyber Security team at one of the biggest Universities in the UK undergoing one of the most exciting digital transformations in the education sector, with cyber security at the very core of our vision.

As the Identity and Access Management Lead you will be accountable for coordinating all activities related to the provision of digital identity services throughout the University, owning services such as Access Management (AM), Identity Governance and Administration (IGA), Multi-Factor Authentication (MFA) and Privileged Access Management (PAM). The University is currently transforming its identity and access management processes. You will support this transformation and become the owner of the underpinning technologies and assurance processes.

You will lead a team dedicated to identity and access management and work collaboratively with teams and stakeholders across the business and third parties. Together the Cyber Security team, you will deliver a cyber security capability fit for a world leading higher education and research institution.

If you thrive working in a highly collaborative, complex, and varied environment this is an exciting opportunity for you to make a real difference in a world class organisation.

Main duties and responsibilities

As the Identity and Access Management Lead your main duties will include:

- Lead the Identity & Access Management service area within the Cyber Security team. You will be responsible and have business ownership for leading the Identity and Access Management strategy and technologies with all associated sub-domains (including but not limited to, MFA and PAM). This will include defining and continuously reviewing IDAM policies;
- Responsible for the ongoing improvement of services and technology that support the staff and student identity lifecycle. This will include engaging with new suppliers to understand the evolving IDAM landscape and how new technologies will enhance or enable the University strategy. Where necessary to improve and develop services and service delivery, you will need to build and manage the approval of business cases for further IDAM funding;
- Manage and Coordinate IDAM technology operational activities (including but not limited to IDAM, MFA and PAM) to ensure high-quality day-to-day operation of the security service. This will include managing the performance of both the internal and external support teams to ensure service levels are met;

- Defining, developing, and managing the IDAM service model, ensuring all necessary service documentation is defined and maintained;
- Coordinate how Identity profiles and personas are managed across IT. This will include, but is not limited to, how services, standards, policies, and processes are designed, introduced, and supported in line with the customer groups of IT.
- Report to the CISO, and wider leadership where necessary, on service performance against quantitative metrics and KPIs including a number of unused accounts, time to provision, etc.;
- Responsible for defining, developing, and coordinating identity and identity related governance groups across the University;
- Build a positive working relationship with your team, internal support teams and third-party suppliers. Support in building a positive team culture and the professional development of the individuals within your team;
- There will be an out of hours aspect to this role, carried out on a rota basis, to support the Cyber Security team in responding to major security incidents or breaches.

These duties provide a framework for the role and should not be regarded as a definitive list. Other reasonable duties may be required consistent with the grade of the post.

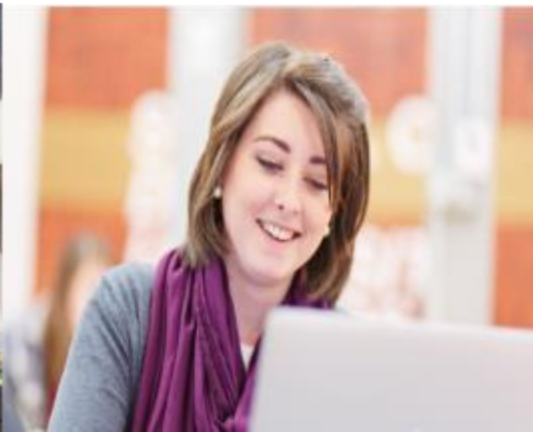
Qualifications and skills

Essential

As Identity and Access Management Lead, you will have:

- Practical experience with Identity and Access Management operations;
- Written and oral communication skills, including the articulation of technical elements of IDAM for business representatives;
- In-depth knowledge of common enterprise Digital Identity lifecycle and service delivery model;
- Expertise of Identity and Access Management concepts including but not limited to - Provisioning, Reconciliation, SSO, Federation, Role-Based Access Control etc.;
- Demonstrate experience of developing and implementing effective standards and strategies that have had a positive impact on service provision;
- Demonstrate experience of effectively leading, managing, motivating, and developing technical teams to improve effectiveness;
- Demonstrate experience of successful resource management including planning, forecasting, monitoring, and reviewing resources.

Key Attributes



- Interpersonal skills and experience developing effective relationships with key stakeholders;
- Demonstrate experience of complex problem solving, making recommendations, and taking into consideration variables to achieve the desired outcomes.

Desirable

- Knowledge of the University application landscape and student lifecycle would be preferred;
- Experience of University Digital Identity Lifecycles advantageous;
- Strong knowledge and experience working with SailPoint, Duo and Thycotic Secret Server & Privilege Manager would be desirable;
- A degree in a technical or computer related subject;
- A CISSP or related cyber security qualification would be advantageous.

Additional information

Find out more about IT.

Our University

At the University of Leeds, we are committed to providing a culture of inclusion, respect and equality of opportunity that attracts, supports, and retains the best students and staff from all backgrounds and from across the world. Whatever role we recruit for we are always striving to increase the diversity of our community, which each individual helps enrich and cultivate. We particularly encourage applications from, but not limited to Black, Asian, people who belong to a minority ethnic community; people who identify as LGBT+; and disabled people. Candidates will always be selected based on merit and ability.

Information for disabled candidates

Information for disabled candidates, impairments or health conditions, including requesting alternative formats, can be found on our Accessibility information page or by getting in touch with us at hr@leeds.ac.uk

How to apply

You can apply for this role online; more guidance can be found on our How to Apply information page. Applications should be submitted by **23.59** (UK time) on the advertised closing date.

Contact information

To explore the post further or for any queries you may have, please contact:

Adam Toulson, Chief Information Security Officer
Email: a.toulson@leeds.ac.uk