Managing multiple-role identities in higher education

Should an adjunct faculty member have access to sensitive data when he is acting in the capacity of a student doing research for a class? Is it appropriate for a university staff member to have the same access entitlements when this individual is doing volunteer work for a club associated with the school? The challenge of managing data access for users with multiple roles, or personas, is especially pronounced within the higher education space. Left unaddressed, colleges and universities may find themselves at risk of breach and regulatory non-compliance.

What are personas and why they matter

Faculty members may also be students. Students may also be staff. Staff may also be volunteers. Having multiple personas per identity makes it extremely difficult to manage users accessing systems, applications and even files containing sensitive data. For instance, should an associate professor also have the same data access levels when he is operating as a student or even a volunteer? To further complicate matters regarding multiple personas, consider the challenges with granting entitlements. For instance, when IT administrators and data stewards make access entitlement changes to a persona, it is not typically applied to other personas. As a result, those changes are either done separately or not done at all. This creates significant inefficiencies as well as cybersecurity and compliance gaps.

Flexibility to meet the unique requirements of educational institutions

Different educational institutions have different requirements and data structures. SailPoint provides multiple ways to meet these requirements. Here are just a few examples of how SailPoint addresses the multiple persona issue:

Persona relationship
This approach is ideal when there is a well-defined authoritative source or application (like HR) for an identity (like an employee). This allows SailPoint to identify a primary identity. SailPoint can also create a primary identity for user types not sourced from HR, such as student accounts and contingent workforce. SailPoint further allows colleges and universities to establish secondary identities that are linked to the primary identity. This allows educational institutions to have a more complete view of the user's access entitlements and enables them to effectively manage their different personas.

Linked relationship persona
Where there are multiple authoritative sources with each being the authority for a different identity persona, the linked-relationship persona approach can be very effective. In this case, SailPoint provides a global identifier where all personas are tied to that individual. Additional personas appear as an application account that are transparently linked back to the main identifier. This model not only builds the relationship but also shows all accesses uniformly.

Roles-based approach
While this is a simpler approach, it is contingent on the environment. Where individuals do not have multiple employee IDs or different managers, personas can be managed via roles. Educational institutions may want to delineate between personas for approvals, certifications, and attestations.

The benefits of the SailPoint solutions

In addition to managing access and entitlements for users with multiple personas, SailPoint solutions can help educational institutions address other cybersecurity and compliance challenges. Here are several examples:

- Colleges and universities typically have a mix of legacy and more current systems and applications. Managing access consistently across all of these technologies can be achieved through SailPoint's unified identity approach.
- SailPoint enables educational institutions to create, manage, and document information access policies and user access rights. This helps educational institutions to confidently meet GDPR and Cyber Essentials Plus regulatory compliance and audit requirements.
- The open culture of education institutions presents a challenge for any cybersecurity program. For this reason, it is important that educational institutions balance security and user productivity by giving the right level of access, at the right time. SailPoint solutions automate formerly manual processes for requesting, granting, and provisioning access through the power of artificial intelligence to deliver more timely, accurate access across the institution.
- SailPoint can extend identity security beyond systems and applications. This allows colleges and universities to find, classify, and control access to data files wherever they reside.

Why educational institutions trust SailPoint

Recognized authority
Many analysts have recognized SailPoint as an identity security leader including Gartner in it's former IGA Magic Quadrant, Forrester's Identity Management and Governance Wave, IDC's Marketscape, and KuppingerCole's Leadership Compass for Identity Governance and Administration.

Consistently high user satisfaction
With a consistent customer satisfaction and retention rating of 95%+, SailPoint is committed to providing a mutually rewarding experience that extends throughout the relationship lifecycle.

Extensive partner network
SailPoint builds strategic partnerships with companies around the world to ensure we have trained sales and delivery partners to best serve our customers.

Technology alliance

SailPoint has broad technology alliances to deliver robust, relevant capabilities that drive strong user experience.

Learn more about SailPoint through one of your peers – The University of Leeds. Get this **article** examining how The University leveraged SailPoint to automate processes such as onboarding or offboarding while putting business leaders in charge of defining identity and role-based access.

About SailPoint

SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.