IDENTITY AUTOMATION

Essential Considerations for Implementing a K-12 Portal

K-12 BEST PRACTICES

Most K-12 districts in the U.S. have seen a dramatic increase in the role of technology across all functions. As such, the need to consolidate the user experience into a single point-of-access has led many to consider launching their own online portals. Below are key areas to consider and when evaluating a K-12 digital ecosystem in preparation for establishing a seamless, secure K-12 portal.

Who is the Portal For?

- Students at all grade levels
- Teachers
- Non-instructional staff
- Substitutes
- Parents/guardians
- Temporary users (contract workers, vendors, visitors, etc.)

What is the Goal of the Portal?

- Provide single sign-on (SSO) access to resources
- Empower the classroom to be more self-sufficient (vs.creating help desk tickets)
- Gain analytical insights into user behavior and ROI on app spend
- Streamline communication between educators and parents
- Secure the digital environment from ransomware attacks
- Reduce IT administrative burden through automation
- Enable the district to govern apps in use and access district data

What Conversations Need to be Had?

- How will you balance user productivity vs. security?
- How will the user experience adapt based on specific needs?
- How will the portal interoperate with your existing systems?
- What self-service options are available to users (ex- reset password)?
- What delegated administration options are available?
- How are resources contained in the Portal provisioned for end users?
- What authentication methods are appropriate for your users?
- Can users authenticate from their devices to access the Portal?
- How granular can your MFA policies be enforced for user groups?
- Can end users initiate access requests through an approval process?

Best Practices for Portal Authentication Security

- Define the systems, apps, and entry points within your digital ecosystem
- Define your various user populations into specific user groups
  - Define authentication methods that are realistic, equitable, and appropriate for each of those user groups
  - Define risk profiles and scores for each user group
  - Determine whether MFA will be automatically required for each user group. If MFA will not be applied to all groups, build in the ability to auto-enforce MFA when a user's risk profile increases until the threat is removed.

! It is essential to include stakeholders from both Information Technology and Instructional Technology teams in these discussions for the most efficient and effective solution. **Remember:** Focus on building a district-wide culture that understands the value of security, communication, and planning!

Contact Us | sales@identityautomation.com | 877.221.8401 | www.identityautomation.com