Password management: best practices

August 28, 2023

There is nothing worse than forgetting your password and being locked out–especially when it's the start of the school year and you have to get right back to work ASAP! We've created the Password Management Best Practices page to help with all your password needs.

We recommend going over the whole page carefully–but here are a few important highlights.

Login redundancies

- We recommend having two distinct highest level operators (District Administrator) for redundancies, in case one operator leaves.
- Consider giving a backup, full-admin rights login to a person who is always onsite, like your principal IT technician. Even if they don't use Alexandria regularly, if you ever get locked out, someone can help.

Emails

- ALWAYS add a valid and current email to an operator patron record so that the operator can recover their password if needed.
- Make sure to whitelist noreply@goalexandria.com, which is the email address any password reset emails will come from. This might need to be done by a district or facility IT team.
- Password recovery when there is no email associated with the user account is a long process, so make sure that all your operator accounts are attached to a valid email address.

Clean up operators

- COMPanion suggests regular audits of who has operator access to Alexandria, and if old operators should be removed. There are multiple security group levels; all may need to be cleaned up. See the associated section on Password Management Best Practices for more details.

We encourage you and your team to make a plan for password management, and feel free to reach out to customer support with any questions at (800) 347-4942 · support@companioncorp.com.

Looking for a Single-Sign-On solution? Alexandria now offers Google SSO! Google SSO is perfect for schools and districts already using Google. Contact our Sales Team if you're interested in adding it to your library!