

Improving security for Universities starts with better passwords

According to the Verizon DBIR 2017 report, 81% of confirmed breaches across the globe were due to weak, reused, or stolen passwords. In Australia, the Office of the Australian Information Commissioner (OAIC) announced that in the June 2018 quarter, the majority of malicious or criminal breaches reported were linked to compromised user names and passwords. For many organisations - universities included - it is a problem that needs to be addressed.

Prioritising the implementation of an Enterprise Password Management (EPM) solution can help universities drive greater cyber awareness amongst staff, faculty and students.

EPM provides greater visibility to security and IT teams into password habits across the university, and enables them to enforce enterprise wide password policy, ensuring best practices are followed.

The Gap that PAM & SSO don't Cover.

While technologies such as two-factor authentication (2FA), web single sign-on (SSO), and privileged access management (PAM) help in reducing reliance on static and easy-to-hack passwords; they don't cover all staff, students or systems, leaving universities still vulnerable to credential theft, password re-use and poor password hygiene.

With a user experience that's loved and trusted by over 13 million people worldwide, LastPass reduces the risk of breach, increases cyber security awareness, and delivers a convenient login experience for all faculty and students that allows them to achieve better password habits.

Comprehensive security controls.

From 100 customisable security policies to detailed reporting logs, the admin dashboard is IT's command central for deploying LastPass campus-wide and strengthening password security throughout the community.

- Admin dashboard
- User and group management
- Policies
- Enterprise MFA options
- Reporting
- Directory integrations
- Federated login with ADFS
- Single Sign-On
- Custom admin permissions
- And more...



All with a zero-knowledge security model.



Federated login for AD



Comprehensive security controls



Secure password sharing



Easy user management and reporting

81% of confirmed breaches across the globe were due to weak, reused, or stolen passwords.

Verizon DBIR 2017 Report

Designed for security first.

We're uncompromising when it comes to data security. User data is encrypted and decrypted at the device level, so that the master password – and the passwords stored in LastPass – are kept secret, even from us. Plus, you can augment security for LastPass accounts with LastPass Authenticator, a leading multi-factor authentication solution with one-tap verification.

Simplified deployment and unlimited support.

LastPass offers streamlined fulfillment tools and educational resources to simplify a campus-wide rollout.

Customised customer success support is provided to ensure you are getting maximum value out of your purchase.

These features deliver the control IT needs and the convenience users expect:

Central admin control

The admin dashboard offers automated user management, policies and more that busy IT admins need.

Federated login with AD

User adoption is easy when you eliminate the separate master password by letting users log in to LastPass with their AD credentials.

User directory integrations

Automate onboarding and offboarding, group management and more with AD, Azure AD, Okta, OneLogin or a custom API.

Secure password sharing

Give teams a flexible, safe way to share access to apps without sacrificing accountability or security.

Detailed security reports

Tie actions to individuals with automated, detailed reporting that helps your business maintain compliance.

100+ security policies

Enforce best practices and control password behavior across the business.

Universal access

Whether in the office, working from home or on the road, employees can securely work anywhere.

Single Sign-On

Federate logins to enterprise-ready cloud apps that live side-by-side in LastPass for a seamless employee experience.

Premium as a Perk

Give a secure, easy way to manage personal passwords with LastPass Premium accounts for all faculty and students.

Visit LastPass.com/enterprise for more information

Visit CAUDIT: www.caudit.edu.au/logmein

Give students, faculty and staff the power to secure their digital life:

- LastPass reliability captures every login, and fills them in during the next visit.
- Remember the master password and forget the rest.
- Whether on a desktop, laptop, smartphone or tablet, accounts are backed up and synced.
- The built-in password generator creates long, randomised passwords that protect against hacking.
- Conveniently and safely share passwords and notes with anyone.

LogMeIn & CAUDIT

Together with CAUDIT, LogMeIn have created affordable packages tailored for Universities across Australia and New Zealand. Provide secure password management with LastPass to every person on campus - students, faculty, and staff.