Why Local Government Can't Afford to Defer Access Security

Security

The digital security landscape for Queensland local government has fundamentally changed. Cyber security is now a continuous operational requirement, underscored by the Queensland Government's 2025-2027 Cyber Security Strategy and the Essential Eight dashboard pilot. This urgency is driven by a concrete threat: Queensland accounts for 28% of all Australian cybercrime reports, with one in eight impacting government entities. Strong access hygiene is the foundation of every mandate, and LastPass makes achieving it attainable.

28%
Australian cybercrime reports occur in Queensland (QLD Cyber Security Strategy 2025).

1 in 8
Queensland cybercrime reports affected state or local government (ReportCyber 2024)

$97,200
Average cost of cybercrime for medium businesses in QLD in 2025, up 55% in one year

47%
of organisations suffered a supply chain attack in 2024

Local councils face a unique trifecta of risk that converges on the user credential:

1. Credential Exposure from Shadow AI and Unmanaged SaaS: Phishing and credential theft are accelerated by staff signing up for unmanaged tools, creating new credentials outside of IT's control—a critical vulnerability for citizen data. LastPass's SaaS Monitoring provides crucial, centralised visibility.
2. Essential Eight Compliance without Security Specialisation: The expanding mandate for Essential Eight compliance is challenging for councils lacking dedicated security teams. LastPass provides enterprise-grade Centralised Password Vaults with enforced Multi-Factor Authentication (MFA) that are simple to deploy and operate, making fundamental controls achievable.
3. The Persistent Risk of Contractor and Vendor Access: The extended supply chain is a significant cyber risk, often involving shared logins and access that persists too long. LastPass solves this with Shared Credential Vaults, allowing secure, temporary access without exposing the actual password, combined with clear audit logs.

© 2026 LASTPASS US LP. ALL RIGHTS RESERVED.

LastPass

For government agencies balancing critical security mandates with constrained budgets, LastPass provides a unique solution. It is IRAP Assessed, ensuring alignment with Australia's security frameworks, and operates with a local Australian team. The IMPACT Program is purpose-built for the public sector, offering cost-efficient, site-wide licensing and included onboarding.

The path to IS18 and Essential Eight compliance is direct, LastPass offers Enforced MFA, Centralised Vaults, SaaS Monitoring, Secure Credential Sharing, and Dark Web Monitoring.

LastPass is the achievable path to strong access hygiene, the foundation upon which all other cyber security mandates must be built.

Request a demo or try LastPass today.

Learn More

© 2026 LASTPASS US LP. ALL RIGHTS RESERVED.

LastPass