

8 Tips to improve your organisation's data security

C U S T O M  D

A

International Law

- ✓ Familiarise yourself with your country's governing principles on privacy:
 - [Australian Rights and Responsibilities](#)
 - [New Zealand Privacy Principles](#)

B

Encryption

- ✓ Introduce a solid information security policy within your organisation to mitigate risk of data leaks and social engineering attacks.
- ✓ Keep your software up-to-date — software vendors regularly release security updates for known vulnerabilities.
- ✓ Use a password manager like [1Password](#)
- ✓ Protect mobile devices like laptops:
 - Use a unique, secure password for your login accounts, and require login after wake from sleep,
 - If you store your users' personal data on such devices, use full disk encryption on [Mac](#) and [Windows](#) where possible.
- ✓ Ask your developers to encrypt users' private data: in the event of a data breach, properly encrypted data is useless to attackers.

C

Minimise Personal Data Collection

- ✓ Having to supply a lot of data is frustrating and time-consuming for users, and with recent publicity about privacy issues it's also likely to make them nervous. Minimising the data you retain also reduces your exposure if something happens. If you don't need really need it, don't collect it.

D

Have A Plan

- ✓ Have a plan in place and ready to deploy quickly in the event of a data breach: your credibility will suffer more if you are seen to be floundering or slow to respond.

