Make data privacy your priority

Mishandling client information can not only cause a financial or reputational loss to the client, it can also lead to a loss of trust and considerable harm to your reputation, loss of customers or business partners and revenue.

Boost your NGR advantage by reviewing and maintaining information security practices.

For over a decade, Growers from across Australia have trusted us to store and maintain their business and contact details.

Privacy and data security is our top priority. Founded on robust processes and systems with the added reassurance that everything is located in Australia.

NGR NATIONAL GROWER REGISTER

1 Outsource your data management with reputable organisations like NGR.

- ✓ Delivers secure, streamlined, simple transactions with clients.
- ✓ Helps ensure your handling of client information complies with legislation such as the Privacy Act*.
- ✓ More efficient internal processes, integrated with existing systems.
- ✓ Eliminates the risk of client data loss or inaccuracies made internally.
- ✓ Reduces risk of privacy breaches.
- Reduces the time & resources involved in addressing any breaches should they occur.

ngr.com.au

How can you keep your data safe?

NGR's systems and practices keep pace with the evolution of data privacy and the ethical use of information. Now, what else can you do?

2 Use strong, unique passwords

- Have procedures to regularly change passwords & user accounts
- Remove users as they move on and require regular password changes to computer access
- Don't share login IDs to access client's personal information – even across your team or business
- Use a reputable password manager service
- Turn off the 'Save Password' feature in web browsers.

3 Use two-factor authentication

- Two-factor authentication might seem like a pain, but it makes your accounts much more secure.
- Two-factor authentication means you need to pass another layer of authentication, not just a username and password, to get into your accounts.
- myNGR requires two factor authentication - back this up with a strong password that you regularly change.

4 Keep work & personal email, online identities & hardware separate

- Keep the online identities and the emails associated with them separate. Avoid using business email addresses for personal activities.
- That way, if a phishing email claiming to be from your 'bank' comes to you work/business email address, you know it's fake.

5 Use passcodes even when they are optional

- Apply a passcode lock wherever available, even if it's optional. Think of all the personal data and connections on your smartphone!

*Find out more at: www.oaic.gov.au

NGR NATIONAL GROWER REGISTER