Dear Participant/Nominee

High Hopes Services is committed to providing our clients with transparency. As part of maintaining this trust and commitment to you, we are reaching out to inform you of a recent security incident involving unauthorised access to our internal systems.

On 3 December 2025, we were made aware of a potential data breach to our company systems. Immediately after High Hopes Services became aware of the data breach, we took immediate actions to secure our systems and prevent any unauthorised access and began an investigation with the help of cyber security experts. The day-to-day operations of High Hopes Services have not been affected, but we wanted to provide you with an update on what has happened and what we are doing about it.

What data may have been accessed?

Our investigation into this incident is ongoing, and we are treating this matter with the highest priority and attention it deserves.

At this stage, our investigation indicates that data within an affected email inbox was accessed and exfiltrated by the malicious actor. We are working to determine the full extent of the information that may have been compromised.

What we are doing

We have:

- secured the affected account, reset credentials and multi-factor authentication was confirmed enabled;
- engaged cyber security experts to investigate the incident;
- notified the Australian Information Commissioner as required in accordance with our regulatory obligations; and
- commenced a comprehensive review of our information security practices and have implemented immediate steps to strengthen our security measures. This review is ongoing, and we remain committed to continuously improving our practices.

What you should do

As a precautionary measure, we strongly recommend you:

Be alert to phishing and scams

- Be cautious of unexpected emails, phone calls or text messages requesting personal information.
- We will never ask for passwords, financial details or sensitive personal information by email or SMS.
- Independently verify the identity of anyone contacting you by calling them back on official numbers.

Monitor your accounts

- Check your bank and credit card statements regularly.
- Review recent transactions and report any unauthorised activity to your bank immediately.

- If you have provided financial information to High Hopes Services, contact your bank to discuss appropriate precautions.

Update your passwords

- Change passwords for any accounts where you may have used the same or similar passwords.
- Use unique, strong passwords (12+ characters, mix of letters, numbers and symbols).
- Consider using a password manager.

Stay vigilant for identity theft

- Be alert to unusual activity such as unexpected bills, credit applications or changes to your accounts.
- Consider requesting a free credit report or placing a temporary credit ban for additional peace of mind.

Protect your personal information

- Be cautious about sharing personal information, particularly health and disability information.
- Verify the identity of anyone requesting your personal details.

Support available

We understand the importance of trust and transparency in our relationship with you. In addition to our immediate response, we have implemented additional safeguards to prevent future incidents If you have any questions or concerns, please don't hesitate to contact our Privacy Team:

- **Email:** admin@hhs.com.au
- **Phone:** 0433 585 367, 1300 556 007 (Monday–Friday, 9 am–5 pm AEDT)
- **Postal:** Director, High Hopes Services, 1/204 Sladen Street, Cranbourne VIC 3977

For general support and guidance, contact **IDCARE**, a free and confidential support service for victims of data breaches and identity theft, at **1800 595 160** or visit **www.idcare.org**.

Stay informed on the best ways to protect yourself by visiting the Australian Cyber Security Centre (ACSC) and the National Anti-Scam Centre's Scamwatch pages:

- **ACSC:** https://www.cyber.gov.au/
- **Scamwatch:** https://www.scamwatch.gov.au/

We will provide you with updates of any significant developments as the investigation progresses. We sincerely apologise for any concern or inconvenience this incident may cause and remain committed to protecting your personal information.

Yours sincerely,

Roby Daou
Director
High Hopes Services