



# EXDIA *express*

*Friendly Updates From Our Team To Yours*

Welcome to *Exdia Express* for April – keeping you informed with friendly updates from our team to yours.

## *In this issue:*

- Team Faces: Meet Angel
- Client Share: Thank you Elizabeth
- ICB eBrief:
  - Changes to Default Super Funds in Awards
  - How Easy is it to Break Passwords?
  - And... ATO Lodgement Dates

We trust you'll enjoy these updates, and we look forward to staying connected!

## ***Team Faces – Meet Angel***



*Bachelor of Science in Accountancy, Certified Public Accountant*

Meet Angel, a key member of the Exdia Bookkeeping team who sees accounting as a stable and rewarding career with significant growth potential. She specialises in financial organization and data analysis, focusing on the efficient and accurate tracking of transactions and account reconciliation. For Angel, being part of the Exdia team is a unique and rewarding

experience, where she plays a crucial role in managing the day-to-day financial transactions of clients. In her spare time, Angel enjoys traveling, exploring new restaurants, and creating daily vlogs to share her experiences.

### ***What do you enjoy most about working with our clients?***

I enjoy working with clients most when I'm able to help with their queries and see them genuinely happy and appreciative of our work—it makes everything feel worthwhile.

### ***What's a simple tip you use to stay productive?***

My simple tip to stay productive is to get enough sleep and plan your day ahead. I like making a to-do list to keep my thoughts organized and avoid distractions.

### ***What's your favourite coffee or snack?***

My favourite coffee is a white chocolate mocha, best paired with cheesy pastries—my go-to comfort combo!

***Thank you, Angel, for being such an amazing part of our Exdia team!***

## ***Client Share – Thank you Elizabeth!***

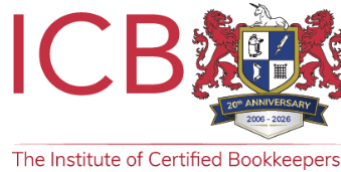
We are so grateful for our wonderful clients, and it's always a pleasure to receive feedback like these thoughtful comments from Elizabeth:

**“You are so committed, experienced, kind, polite, generous with your time, servant hearted and a pleasure to work with.” – Elizabeth, NSW**

Thank you, Elizabeth, for sharing your experience. We truly value the opportunity we've had to work together!

And now in the following section we are delighted to share the latest eBrief from the Institute of Certified Bookkeepers with this month's topics and content.

## Client eBrief



## Changes to Default Super Funds in Awards

### Award Super Funds Updated

The Fair Work Commission has updated 125 modern awards to reflect changes in the superannuation industry.

Over time, some awards have included super funds that have merged, closed, or changed names. This created inconsistencies between the award wording and the funds that actually operate today.

This review was carried out to ensure the default fund lists in awards remain accurate and up to date.

### What Has Changed

**Old fund names were removed:** Some default funds listed in awards no longer exist in their original form. These names have now been removed.

**Current fund names were added:** Awards now list the correct, active super funds that employees can be paid into if they do not nominate their own.

**The default fund lists are now consistent:** This helps reduce confusion for payroll teams and employers when setting up new employees.

## ATO Lodgement Dates

These dates are from the ATO website and do not account for possible extensions.

You remain responsible for ensuring that the necessary information is with us in time.

See [ATO Due dates by month](#) to check monthly lodgment and payment dates.

### BAS/IAS Monthly Lodgements

Final dates for lodgements and payments:

March Activity Statement  
21 April 2026

April Activity Statement  
21 May 2026

### BAS Quarterly Lodgements

Final dates for lodgements and payments:

**3rd Quarter 2026 Financial Year:**  
**March Quarter 2026 (incl. PAYGI)**  
28 April, 2026

**4th Quarter 2026 Financial Year:**  
**June Quarter 2026 (incl. PAYGI)**  
28 July, 2026

When a due date falls on a Saturday, Sunday or Public Holiday\*, you can lodge or pay on the next business day.

\*A day that is a public holiday for the whole of any state or territory in Australia.

Due date for super guarantee contributions:

**3rd Quarter 2026 Financial Year:**  
January to March 2026 – contributions must be **in the fund** by 28 April, 2026

**4th Quarter 2026 Financial Year:**  
April to June 2026 – contributions must be **in the fund** by 28 July, 2026

Late payments of superannuation are **not** tax deductible. If your business has overdue superannuation guarantee payments and you are unsure of how to proceed, please contact us to discuss.

**No change to super obligations:** There has been no change to Super Guarantee rates, employer obligations, or payment timing. This update only affects fund names.

Nothing else in the superannuation clauses of awards was altered as part of this process.

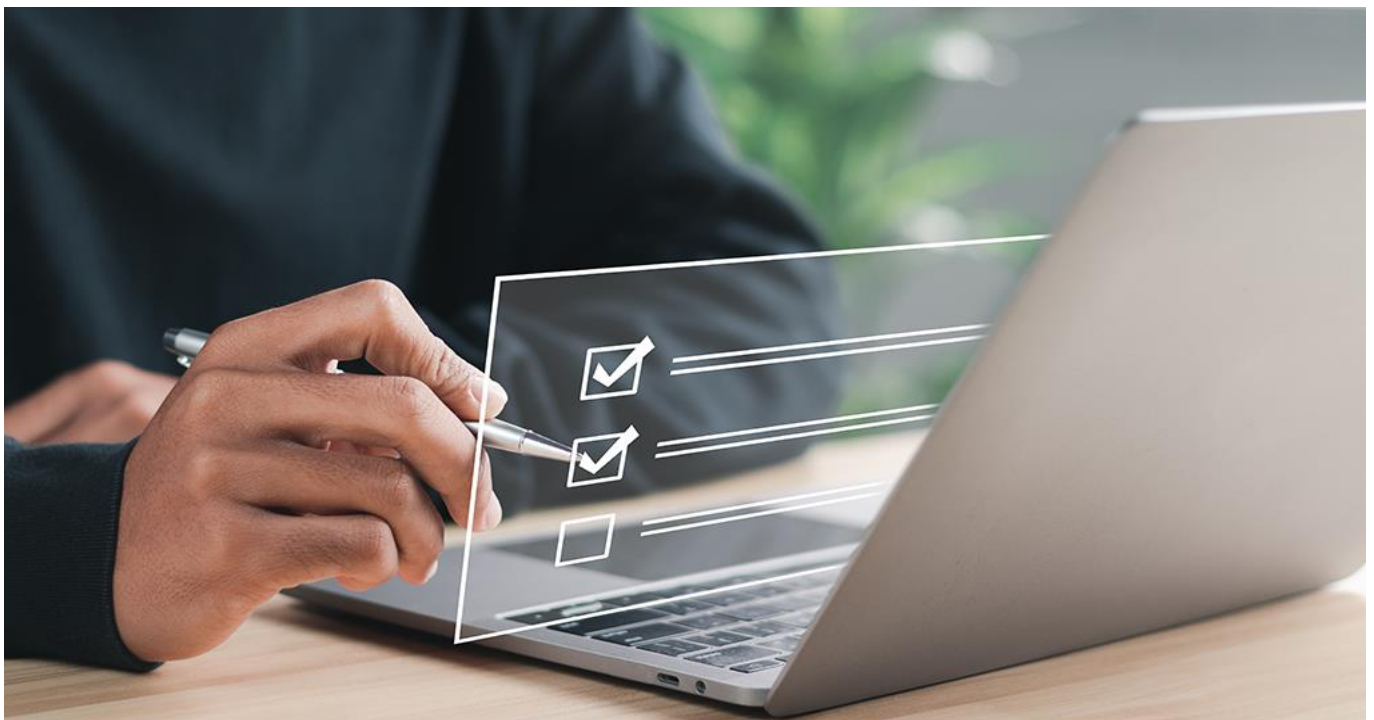
### What This Means for Business Owners

For most businesses, this change will not affect how super is calculated or paid. It simply means the default super fund listed in some awards may now appear under an updated or different name.

If an employee does not choose their own fund, the employer must still use the default fund listed in the relevant award. Because some fund names have been updated, it is a good time to check that your onboarding documents, employment contracts, and payroll software reflect the current fund names used in the award.

Your bookkeeper can help review payroll settings, confirm that the correct award default fund is being used, and ensure any outdated fund names are updated in your records. This helps avoid confusion when setting up new employees and ensures super contributions are directed to the correct, active fund.

**Source:** [Changes to default super funds in awards - Fair Work Ombudsman](#)



## How Easy is it to Break Passwords?

### Why You Should Use Longer Passphrases & MFA

Cybersecurity threats continue to rise. The Australian Cyber Security Centre (ACSC) Cyber Threat Report 2024-25 highlights that weak or stolen passwords remain one of the most common entry points for attackers. Whether you are managing your accounts, using cloud software, or running day-to-day business systems, short and simple passwords offer very little protection against modern cyber-attacks.

**Harvey Norman**  
TECHNOLOGY FOR BUSINESS

## How Quickly Can a Password Be Cracked?

Cybercriminals often use brute force and dictionary attacks to guess passwords. A brute force attack systematically tries every possible combination of letters, numbers, and symbols until it finds the correct one. Advances in computing power have made these attacks incredibly fast. Here's how quickly modern hacking tools can break passwords, based on the latest Hive Systems 2025 Password Table:

| Password Length | Complexity (Lowercase Letters Only) | Complexity (Mixed Case, Numbers, and Symbols) |
|-----------------|-------------------------------------|---|
| 4 characters    | Instantly                           | Instantly                                     |
| 6 characters    | Instantly                           | Instantly                                     |
| 8 characters    | Less than 8 seconds                 | 8 hours                                       |
| 10 characters   | 4 minutes                           | 3 weeks                                       |
| 12 characters   | 2 hours                             | 300 years                                     |
| 16 characters   | 1 month                             | 25 trillion years                             |

These statistics highlight a simple fact: short passwords are not secure.

If you use passwords shorter than 12 characters, your sensitive data could be at serious risk.

## Why Should You Use Longer Passphrases?

A passphrase is a longer, more complex password that consists of multiple words strung together, making it both stronger and easier to remember. For example, instead of using "Passw0rd!", which can be cracked in seconds. Try combining unrelated words with a symbol, e.g., "BluePiano\$TigerMountain."

Here are some benefits of using passphrases:

- **Increased Security** – 16+ characters make brute force attacks nearly impossible.
- **Easy to Remember** – A sentence-like phrase is simpler to recall than a random mix of characters.
- **Lower Risk of Reuse** – Employees tend to reuse short passwords across multiple accounts, which makes them vulnerable if one account is compromised.

## Benefits of Using a Password Manager

Managing multiple passwords is one of the biggest challenges for businesses. Employees often struggle to remember complex credentials, leading to bad habits such as writing them down or reusing the same password across accounts. A password manager solves this problem.

While password managers significantly improve security, they are not perfect. Like any risk mitigation strategy, businesses must weigh the risks against the benefits. Strong passwords are essential, but they are only one piece of a broader cybersecurity strategy, and this is where partnering with a technology solutions and security provider (TSSP) becomes valuable.

## Combining a Strong Passphrase with Multi-Factor Authentication (MFA)

Relying on a password alone, even a strong one, is no longer considered enough to protect sensitive data. Hackers have powerful tools that can quickly guess passwords, and stolen passwords are common in data breaches. That's why a long, unique passphrase is a great first step, but it

shouldn't be your only defence. Adding multi-factor authentication (MFA) makes your accounts much harder to break.

This extra layer means even if someone steals your passphrase, they still can't get in easily, significantly reducing your risk. By combining a strong passphrase with MFA, businesses can protect against common attacks such as phishing and password-guessing. It's one of the simplest and most effective ways to keep your business safe.

## Working with a Technology Services and Security Provider (TSSP)

Cybersecurity can feel overwhelming, especially for busy practice owners, clinic managers, and small business owners, including sole traders, who are focused on delivering services, not managing IT systems. Navigating the complexities of commercial level cyber security can be overwhelming. A technology services and solutions provider offers the expertise needed to assist business owners in managing their cybersecurity needs effectively.

By partnering with a technology services and security provider, businesses can leverage advanced security measures without an in-house team. This ensures that the business's digital assets are well-protected and compliant, allowing the business to focus on what's important.

That's where a Technology Solutions and Services Provider (TSSP) comes in. A TSSP provides expert guidance, tools, and ongoing support to help businesses implement and maintain robust cybersecurity measures, including the Essential Eight strategies recommended by the Australian Cyber Security Centre.

## How Harvey Norman Technology for Business Helps

Harvey Norman Technology for Business specialises in complete IT solutions that enhance cyber security, protect critical data, and maximise the efficiency of your IT systems, specifically designed for all businesses, including sole traders.

- **Simplified IT:** Enterprise-grade solutions, secure networks, and expert technology services made easy and stress-free.
- **Proactive Protection:** 24/7 monitoring, real-time threat detection, compliance-ready security, and preventative system maintenance.
- **Cyber security:** Secure backups, recovery management, advanced threat protection, and rapid incident response.
- **Local Expertise, Nationwide Support:** Access to a world-class help desk, backed by personalised service and the support of a trusted national brand.

HNTB understands the challenges of staying ahead of evolving cyber threats, complying with regulations, and maintaining optimal IT performance. Their goal is to assist businesses in safeguarding sensitive business data, minimising risk, enhancing system efficiency, and staying protected.

Here's how they can support business:

- Advanced cyber security solutions to protect against emerging threats.
- Insights on Australian laws and regulations.
- Proven strategies to secure sensitive financial and customer information.
- Best practices for security, compliance, and risk management.
- Proactive management of your IT system environment, reducing risk and ensuring optimal performance.

- Help desk support for all IT-related issues.
- 24/7 monitoring by an expert security team.

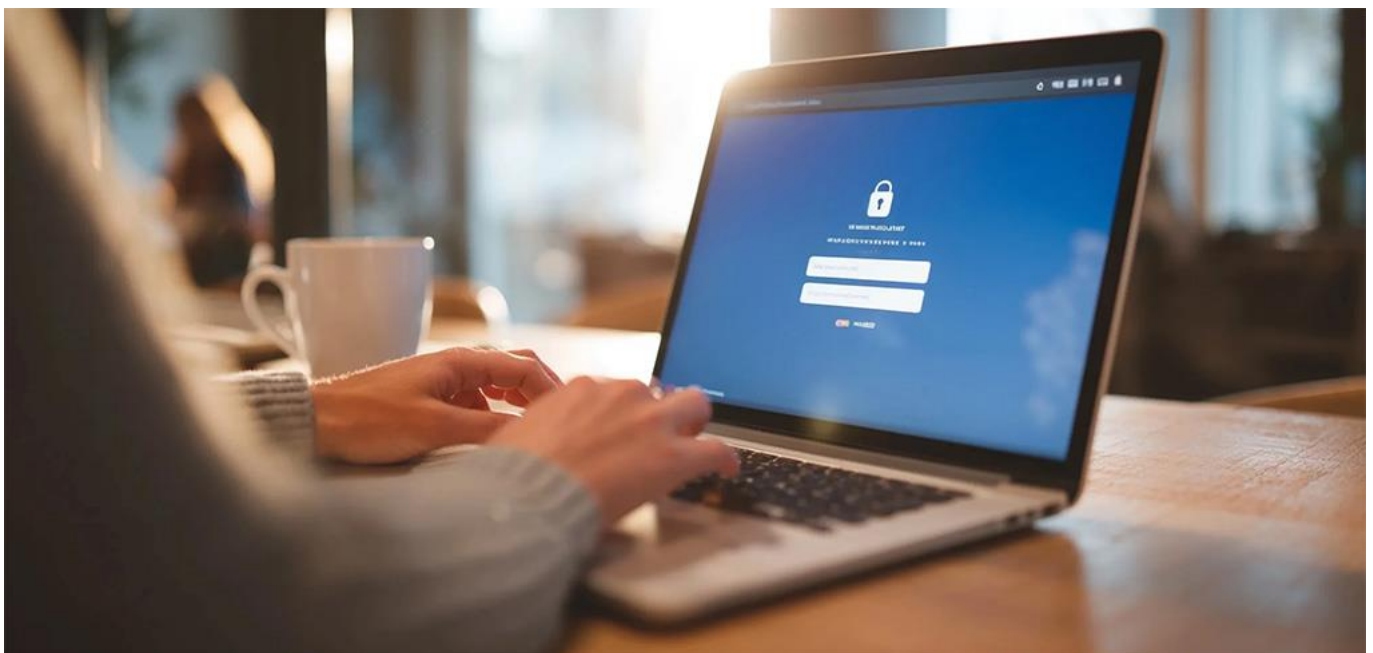
Harvey Norman Technology for Business is a trusted ICB partner, empowering business owners with cybersecurity and technology solutions to keep their business safe, secure, and ready for growth.

## Conclusion

Cyber threats aren't just a concern for large businesses. Whether you have 0 employees or over 300, hackers know smaller businesses often have weaker security measures, making them prime targets. According to the ASD Cyber Threat Report 2024-25, cybercrime reports have increased 23%, and the average cost of an incident for small businesses is now over \$56,000. That's a cost most businesses cannot afford.

Implementing simple steps, such as using strong passphrases and a password manager, can drastically reduce your risk. Add Multi-Factor Authentication (MFA), and you have built a powerful defence against common attacks like phishing and credential theft. Protect your business with Harvey Norman Technology for Business. We make enterprise-grade cybersecurity simple, affordable, and designed for small to medium-sized businesses and sole traders.

[\[Read Full Article\]](#)



Disclaimer: All or any advice contained in this newsletter is of a general nature only and may not apply to your individual business circumstances. For specific advice relating to your specific situation, please contact your accountant or contact me for further discussion.

**The Institute of Certified Bookkeepers**

Tel: 1300 856 181

Email: [admin@icb.org.au](mailto:admin@icb.org.au)

This newsletter is produced by the Institute of Certified Bookkeepers and distributed by members.

