PRESS RELEAS: FOR IMMEDIATE DISTRIBUTION

More Than Half of Australian Executives Are Feeding Confidential Data Into AI. The Fix Is Security Built In From the Start.

Australian AI workforce platform WorkClone commissioned independent research after seeing the problem firsthand inside Australian boardrooms. The findings confirmed what the company was founded to fix.

New research, conducted by Primara Research, reveals a concerning trend at the top of Australian organisations: executives are the most likely to input sensitive information into AI tools, yet 99% know exactly what qualifies as sensitive data. The nationally representative survey of 1,000 Australian workers found 55% of executives admit to entering sensitive data into AI tools, compared with 49% of managers and 36% of employees.

The people who know better are doing it more

Executives also report the highest concern about data exposure through AI, with 80% flagging it as a risk. Yet more than one in five (21%) are unaware that consumer AI tools store and use their inputs, and only 45% have a firm understanding of how AI data training actually works.

"Executives handle the most sensitive information in any organisation, including financials, strategy and client data," said Natalie Ashes, CEO of WorkClone. "Data entered into publicly available AI tools may be stored on overseas servers, used for model training, or accessible to the platform provider under terms most users have never read. For ASX-listed companies that can carry disclosure obligations. For professional services firms, it can breach client confidentiality clauses. For anyone handling personal information, it may violate the Privacy Act."

AI software built for business must have security baked in from the start. That is the principle WorkClone was founded on, deploying agentic AI agents in secure, isolated environments with enterprise-grade governance, giving businesses a way to use AI productively without exposing sensitive data to public systems, with full auditability and human oversight built in from day one.

Medium businesses are the most exposed

The risk is sharpest in medium-sized businesses (50-200 employees), where 50% of workers admit to entering sensitive data into AI, including 16% who do so regularly. Large businesses sit at 45% (12% regularly), while small businesses show the lowest rates at 35% (8% regularly).

Formal AI policies help explain the divide: 56% of large businesses have one, versus 43% of medium, but just 25% of small. Yet despite that gap, small businesses still record the lowest rates of sensitive data entry (35%), suggesting personal accountability fills the void where policy doesn't exist. Medium businesses, caught between the two, fare worst when it comes to entering sensitive data into AI.

"Medium businesses have outgrown the personal accountability that keeps small teams in check, but haven't yet built the governance infrastructure of a large enterprise," said Ashes. "That's exactly where data leaks quietly through the cracks, and exactly the market we are expanding into."

AI usage is no longer a niche workplace behaviour. Ninety percent of employees now use AI tools, with 74% doing so weekly, meaning the volume of data flowing into these platforms is significant and growing. The question for every business is not whether their people are using AI, but whether the tools they have chosen were built to handle what is going into them.

The People Behind WorkClone

CEO Natalie Ashes began her career in technology before moving into senior commercial and marketing leadership. She is recognised as a top Executive Leader of the Year and ranked among Australia's top marketing and tech executives, with a track record of scaling digital ventures and building high-performing product and growth teams.

CTO Oliver Shanahan was part of the founding technology team behind BetMakers, the wagering technology platform that grew into ASX-listed BetMakers Technology Group. Building technology in one of Australia's most heavily regulated industries, where a single data failure can end a business, meant security was never optional. WorkClone was built with that same discipline from day one.

“If an AI agent is going to speak to customers, touch systems or handle sensitive information, security can't be a slide at the end of the deck. It has to be the architecture."

WorkClone recently completed a funding round and is expanding from enterprise into mid-market clients, the same segment the research identifies as most at risk, through delivery models designed to get AI agents operational within weeks rather than months.

Clone Your Best People

WorkClone's answer to that question starts with a different premise altogether. Rather than asking businesses to restrict AI use, it gives them a secure, governed alternative: AI agents modelled on the knowledge, communication style, and decision-making patterns of their best operators, deployed to handle the repeatable work so the original can keep doing what makes them irreplaceable.

"Every business has people who are genuinely brilliant at what they do," said Ashes. "But too often they're drowning in work that a well-built AI agent could handle. We clone those people, not to replace them, but to multiply them."

The application is broad. After-hours client communications. Recruitment screening. Operational triage. Knowledge management. These are exactly these use cases that illustrate why security cannot be optional. The survey found 30% of AI users are already entering customer and client data into unprotected tools, making governed, isolated environments, like WorkClone, not a nice-to-have, but a baseline requirement.

A Different Kind of AI Company

WorkClone's agents are already live with business customers across financial services, recruitment and professional services, supporting high-volume customer interactions, after-hours service and workflow triage in regulated environments where security and compliance matter. In practice this means extending operations into a 24/7 model without adding equivalent headcount.

WorkClone's pitch to the market is deliberately contrarian.

In an era where AI adoption is most commonly framed around headcount reduction, WorkClone argues the more valuable opportunity is different: use AI to protect and multiply your best people, not eliminate your average ones.

"We're not building tools to replace your team," says Ashes. "We're building tools so your team can stop doing things machines are better at. The humans still need to exist, and in our model, they're more valuable, not less."

About WorkClone

WorkClone is an AI workforce platform that deploys secure, role-based AI clones of top employees. Each clone is built from real workflows, approved company knowledge, business rules, communication style and decision-making patterns, then deployed inside secure, isolated environments with enterprise-grade governance.

workclone.com

About The Research`

The research was conducted by Primara, an independent Australian consumer and business research company. 1,000 Australian workers were surveyed in April 2026.

Media Contact

Natalie Ashes CEO, WorkClone [email] [phone]


workdone