PRACTICAL GUIDE

AI Safety Checklist

Enable AI safely, securely, with customer trust. A practical guide for business leaders and startup founders in Singapore.

AI is powerful. It can help you move faster, serve customers better, automate the work that slows you down. But most businesses adopt AI tools without any policy, oversight or understanding of where their data goes. You would not give a stranger unsupervised access to your customer database, your finances and your email. That is essentially what happens when you connect an AI tool without checking what it can access. This checklist gives you 22 practical steps. No technical knowledge required. Ten minutes to read. Share it with your team.

WHO IS THIS FOR

Startup founders	using AI to build products, serve customers or run operations.
Small business owners	who have staff using ChatGPT, Copilot or automation tools.
Home businesses	using AI for marketing, invoicing, customer service or content creation.
Anyone in Singapore	deploying AI without a dedicated security or compliance team.

14.5%
SME AI ADOPTION RATE
Tripled from 4.2% in one year. Large enterprises at 44%.

3rd
SINGAPORE RANKS 3RD GLOBALLY
for exposed AI agent instances.

43%
OF PUBLIC AI AGENT SERVERS
are vulnerable to remote exploitation.

HOW TO USE THIS CHECKLIST

1 Read it.
Ten minutes. That is all it takes.

2 Score yourself.
Tick what you already do. Count the gaps.

3 Pick three.
Start with the three that matter most. Do not try to fix everything at once.

4 Share it.
Give a copy to your partner, your team and anyone who touches AI.

BEFORE YOU START

1. Read the terms of service
Does the provider use your data to train their models? If yes, do not paste anything confidential.

2. Ask where your data goes
Which country is it stored in? Who can access it? Can you delete it? If they cannot answer, do not use it.

3. Test with fake data first
Run the tool with made up information. Check outputs for errors and fabrications before connecting real data.

4. Decide what it must never do
If AI should never quote prices, make legal claims or promise delivery dates, write that down and tell your team.

5. Check who owns what AI creates
If you use AI to write content, code or designs, check the terms. You may not own the intellectual property.

6. If the model is free, ask why
Free AI tools often monetise your data. If you are not paying for the product, your data is the product.

7. Assign a human reviewer
Every piece of AI content that reaches a customer must pass through a person first. No exceptions.

8. Pilot with one team first
Roll out to a single team before the whole company. You will spot problems quickly with low blast radius.

AFTER YOU DEPLOY

9. Check outputs weekly
Schedule a review. Look for errors, drift and patterns that do not match expectations.

10. Keep an error log
When AI gets something wrong, write it down. What you asked. What it said. What was wrong.

11. Tell your customers
If AI generates any part of their experience, let them know. Transparency builds trust.

12. Have a kill switch
Know how to turn off any AI tool in minutes. Not hours. Minutes.

13. Review every quarter

AI tools update constantly. What worked three months ago may behave differently now.

14. Train your team

Five minutes of training on what AI is and is not for prevents most mistakes. Show your team the kill switch.

PROTECT YOUR DATA AND YOUR PEOPLE

15. Handle personal data with extreme care

If your AI tools process customer names, emails, phone numbers or financial data, you must follow Singapore's PDPA. The fines are real.

16. Do not install AI on your banking machine

Keep experiments separate from production. If the tool gets compromised, the attacker gets everything on that machine.

17. Only download from trusted sources

Official app stores and known vendors. Not forum links, not shortcut URLs, not messages from strangers.

18. Know what your AI agents are doing

AI agents download code and connect to systems without asking. Singapore ranks 3rd globally for exposed instances. Check permissions.

AS YOUR STARTUP GROWS, SO DOES YOUR RISK

19. More customers, more data liability

What works for 100 customers may not be compliant at 10,000. Reassess as you scale.

20. More tools, more attack surface

Every AI agent you add is another door. Make sure each one is locked.

21. Regulators are watching

Singapore's CSA and PDPC are publishing new AI guidance in 2026. Stay ahead of it.

22. Get cyber insurance fit for AI

Most policies exclude unauthorised software. As you scale, get coverage that explicitly includes AI tool breaches.

SINGAPORE HAS YOUR BACK

IMDA GenAI Starter Kit
Free AI sandbox for Singapore businesses.
imda.gov.sg

PDPC Data Protection Guidelines
How to handle customer data when using AI.
pdpc.gov.sg

CSA AI Security Guidelines
Updated in 2026 with agentic AI guidance.
csa.gov.sg

IMDA Agentic AI Governance Framework
World's first framework for AI agents. Launched January 2026.
imda.gov.sg

Enterprise SG GenAI Navigator
Pre approved AI with government grants up to 70%.
enterprisesg.gov.sg

AI Verify Foundation
Open source AI testing toolkit. Test models for safety and fairness before deployment.
aiverifyfoundation.sg

HOW DTN ADVISORY CAN HELP

AI Risk Assessment
Evaluate your AI tools, agents and data flows. Identify what is exposed and what needs to change.

Security Strategy
Build a cybersecurity posture that works under pressure. Board level advisory and operational support.

Incident Readiness
Prepare your team for when things go wrong. Tabletop exercises, playbooks and response planning.

Compliance and Governance
Navigate Singapore's PDPA, CSA guidelines and international AI governance frameworks.

WANT TO LEARN MORE?

Visit dtnadvisory.com or read the full articles on dtnadvisory.substack.com · connect@dtnadvisory.com

YOUR SCORE

Score: ___ / 22 Date: _____

0 to 8: High risk. Start now. **9 to 16:** Making progress. Close the gaps. **17 to 22:** Strong position. Keep reviewing.

Stats based on publicly available SME AI adoption surveys, Censys AI agent exposure research and CSA vulnerability disclosures (2025/2026).