

Position Paper 2026:

Trust and Safety – Securing Aotearoa's Digital Prosperity

Executive Summary

As TUANZ marks 40 Years championing a brighter digital future for every New Zealander, we can be quietly confident that we are making progress building a resilient digital foundation for our country. The successful integration of CERT NZ into the National Cyber Security Centre (NCSC) and the success of initiatives like Malware Free Networks (which disrupted over 10.3 million malicious events last year) demonstrate that we are on a journey to improve our national capability to defend our digital borders.

Aligning with our 2026 Action Plan, TUANZ believes that Trust and Safety are the bedrock of our digital future. By securing our digital environment, we unlock immense national benefits: we address the \$200 million New Zealanders lose annually to scams, foster the social licence required to adopt high-value AI, and ensure our \$17 billion tech sector can compete globally with confidence. We advocate for a shift from "user beware" to a proactive national strategy where safety is built-in, and the "cyber equity gap" for small businesses is finally closed.

The Current Landscape

New Zealand's digital environment is currently at a crossroads of significant achievement and evolving complexity.

- **Defensive Capability:** Our lead agencies are delivering results, with the NCSC preventing an estimated \$38.8 million in harm to nationally significant organisations in the 2023/24 year.
- **The AI "Double-Edged Sword":** While AI offers enormous productivity gains, it has also lowered the barrier for entry for bad actors. Scammers now use Generative AI to craft realistic, personalised phishing attacks that are increasingly difficult for users to distinguish from legitimate communications.
- **The Widening Equity Gap:** A dangerous disparity has emerged; while large organisations are fortifying their defences, 35% of small organisations believe their cyber resilience is now insufficient and this figure has increased sevenfold since 2022.

Our Position

TUANZ stands as the strong independent voice for users navigating a digital world. We assert that Cyber Security and Online Safety are essential national infrastructure. Just as the government ensures the safety of our physical roads, it must lead the coordination of a safe digital environment.

Consistent with our Action Plan for 2026, our position is that Aotearoa must move toward a "Security by Design" philosophy. We believe that trust is earned when safety is an inherent feature of digital services, not an optional extra. We advocate for a whole-of-ecosystem approach where government leadership provides regulatory certainty, platforms are held accountable for the content they host, and every New Zealander is empowered with the skills to remain safe online.

Recommendations for Action

To secure Aotearoa's digital prosperity and ensure a safe environment for all, TUANZ recommends the following four actionable steps:

- **Develop an Enforceable National Cyber Security approach:** The Government should transition from voluntary guidelines to enforceable legislation. This must include mandatory reporting for major cyber-attacks and enhanced capabilities for agencies to investigate and prosecute global cybercriminals targeting New Zealanders.
- **Close the SME Gap with "Cyber Health Incentives":** To bridge the equity gap, the Government should introduce incentives for Small to Medium Enterprises (SMEs). This could include tax rebates or direct grants for adopting essential security "hygiene" such as multi-factor authentication (MFA) and secure cloud backups.
- **Mandate Platform and Provider Accountability:** We call for regulation that requires telecommunications and social media platforms to proactively detect and block fraudulent activity and deepfakes. The burden of identifying sophisticated AI-generated scams need to shift from the individual user to the providers of these networks.
- **Embed Cyber Safety as a Core Life Skill:** We must treat digital literacy as being as important as reading and mathematics. The Government should mandate technology upskilling in the school curriculum, ensuring the next generation enters the workforce with the critical thinking skills to identify AI-driven misinformation and protect their digital identities.

Conclusion

A safe digital Aotearoa is a prosperous Aotearoa. By treating Trust and Safety as a national priority, we do more than just prevent harm; we create a competitive advantage that attracts global investment and empowers our citizens to embrace innovation without fear. The exponential growth of AI-driven threats means we can no longer rely on reactive measures. By implementing enforceable standards and closing the SME gap, we can ensure that New Zealand remains a world-leading, trusted digital nation. TUANZ is committed to championing this brighter, safer future for every New Zealander.

