DRAFT

Code of Practice for the Inclusive and Ethical Use of Digital Identity

19 November 2024

Introduction

In today's digital world, identity Is no longer limited to physical documents or face-to-face interactions. Now, our identities are largely digital, existing in online spaces. New Zealand is committed to embracing the opportunities digital identity brings while protecting the rights, privacy, and security of all its citizens. The Digital Identity Services Trust Framework Act 2023 (DISTF) reflects this commitment, offering a blueprint for secure, inclusive and ethical digital identity practices.

The DISTF provides a clear set of principles, standards and best practices that guide organisations and individuals in digital identity use. It's all about fostering trust, inclusivity, privacy protection, data security, and fairness in every aspect of digital identity management.

On a global level, the OECD's Recommendation on the Governance of Digital Identity encourages developers of digital identity systems to focus on accessible, ethical, and equitable solutions that truly serve users' needs.

In alignment with both the DISTF and the OECD guidelines, the Inclusive and Ethical Use of Digital Identity (IEUDI) Code of Practice sets a standard for responsible digital identity practices in New Zealand. This code, created by the IEUDI Working Group within Digital Identity New Zealand (DINZ) – the leading voice for digital identity in Aotearoa – invites individuals and organisations to actively contribute to a more inclusive, resilient, secure, and equitable digital society.

This code is a work in progress, shared to spark reflection and dialogue. Together, lets shape a future where digital empowers and respects the rights and dignity of all people in New Zealand.

Code of Practice for the Inclusive and Ethical Use of Digital Identity

Purpose

This code of practice is intended to guide organisations and individuals in the responsible and ethical use of digital identity information. It aims to promote inclusivity, security, privacy and fairness in all digital identity-related activities.

Principles

1. Respect for privacy

a. **Consent:** Always obtain explicit and informed consent from individuals before collecting, storing, or using their digital identity information.

b. **Minimisations:** Collect only the minimum amount of digital identity information necessary for the intended purpose.

c. **Data Security:** Implement robust security measures to protect digital identity data from unauthorised access, breaches, or misuse.

d. **Transparency:** Clearly communicate how digital identity data will be used and provide access to privacy policies.

2. Inclusivity

a. **Accessibility:** Ensure digital identity solutions are accessible to all individuals, regardless of disabilities or limitations.

b. **Diversity:** Avoid discriminatory practices that may exclude or disadvantage any group based on race, gender, age, disability, or other protected characteristics.

c. **Interoperability:** Promote standards that enable different digital identity systems to work together seamlessly.

3. Meaningful engagement with Māori:

a) **Establish a structured, early and ongoing consultation** with Māori communities, involving hui and other culturally appropriate forums to gather input and feedback

b) **Actively seek the involvement of Māori representatives**, leaders or advisors in decision-making bodies related to the design, development and governance of digital identity systems
c) Placeholder: Alignment with the DINZ te Tiriti SOI and Action Plan when this is completed.

4. Accuracy and Integrity

a. **Data Accuracy:** Strive for accuracy in digital identity data and provide mechanisms for individuals to correct inaccuracies.

b. **Data Quality:** Maintain the integrity of digital identity data throughout its lifecycle.

5. Security and Protection

a. **Cybersecurity:** Implement state-of-the-art cybersecurity measures to safeguard digital identity information.

b. **Identity Theft Protection:** Educate individuals about the risks of identity theft and provide resources to mitigate such risks.

c. **Data Breach Response:** Establish a clear plan for responding to data breaches and notify affected individuals promptly.

6. Ethical Considerations

a. **Non-Discrimination:** Do not use digital identity information to discriminate against individuals or groups.

b. **Consent Withdrawal:** Allow individuals to withdraw their consent and delete their digital identity data upon request.

c. **Accountability:** Hold organisations and individuals accountable for unethical or illegal use of digital identity data.

7. Education and Awareness

a. **Public awareness:** Promote public awareness about digital identity concepts, risks, and best practices.

b. **Training:** Provide training and resources to employees and stakeholders to ensure compliance with this code of practice.

8. Continuous Improvement

a. **Feedback:** Encourage feedback from individuals and stakeholders to improve digital identity practices.

b. **Periodic Review:** Regularly review and update digital identity policies and practices to stay aligned with evolving technologies and ethical standards.

9. Legal Compliance

a. **Compliance:** Ensure compliance with the DISTF Act 2023, the Privacy Act 2020, and with other relevant data protection laws and regulations as appropriate such as the European GDPR.

b. **Ethical Standards:** Go beyond legal requirements to adhere to higher ethical standards in digital identity management.

10. Reporting and Accountability

a. **Reporting Misuse:** Encourage individuals to report any misuse or unethical practices related to digital identity.

b. **Accountability:** Hold individuals and organisations accountable for violations of this code of practice.

Declaration

By adopting this Code of Practice, we commit to fostering an inclusive, secure and ethical digital identity ecosystem that respects the rights and dignity of individuals. We believe that through these principles, we can contribute to a more equitable and trustworthy digital world.

[Organisation name]

[Signatory]

[Date of Adoption]

Appendix: Future considerations

This Appendix briefly introduces additional considerations discussed by the DINZ Inclusive and Ethical Use of Digital Identity (IEUDI) Working Group in the course of developing this draft IEUDI Code. Its aim is to provide the reader with a sense of the range of directions it could extend, upon successful adoption as a voluntary initiative.

1) An approach to monitoring adoption and participation in a voluntary code of practice

To guarantee the ethical and inclusive implementation of the Code of Practice for Digital Identity Services, it is advisable to establish a dedicated oversight body. This regulatory entity should possess the authority to supervise, monitor, and report on service providers' compliance with the code. To instil confidence in consumers regarding the maintenance of ethical standards, the oversight body should publicly disclose the names of participating organisations. The recommendations and considerations for this body include exploring the possibility of broadening the scope of existing groups or creating a distinct, independent entity. The proposed structure and empowerment of this body could be designed as follows:

a. Formation of the Monitoring Body:

The monitoring body shall be an independent entity established by the relevant government authority (in this case DIA) responsible for digital identity services oversight. It should consist of experts with diverse backgrounds, including technology, privacy, ethics, and legal expertise.

b. Scope of Authority:

The regulatory body should have the authority to oversee and monitor compliance with the Code of Practice. This includes the ability to investigate potential violations, issue guidelines, and provide education and support to non-compliant service providers.

c. Monitoring and Assessment:

The regulatory body should regularly monitor and assess the performance of service providers in relation to the Code of Practice. This may involve conducting audits, collecting data, and soliciting feedback from users and stakeholders.

d. Collaboration and Education:

The regulatory body should work collaboratively with industry stakeholders and the service providers to promote understanding and adoption of the Code of Practice. It should provide guidance and educational resources to help service providers comply.

e. Transparent Reporting:

The regulatory body should issue regular reports in the public domain summarising its activities, including compliance assessments, while respecting privacy and security considerations.

f. Appeals Process:

Service providers should have the right to appeal decisions and reporting from the regulatory body. An independent appeals process should be established to ensure fairness and due process.

g. Adequate Resources:

The regulatory body should be adequately funded and staffed to carry out its responsibilities effectively, and its funding should be secured independently to avoid conflicts of interest.

h. Continuous Improvement:

The regulatory body should be committed to continuous improvement, adapting to changing technologies, evolving risks, and emerging best practices in the field of digital identity services.

By establishing such a monitoring body with clear authority, resources, and monitoring mechanisms, we can ensure that the Code of Practice is more than a set of principles—it becomes a meaningful and effective tool to promote ethical and inclusive use of digital identity services while safeguarding user rights and privacy. This will ultimately foster trust and confidence in the digital identity ecosystem.

2) Transitioning from a voluntary to a mandatory code of practice

This summary document proposes the adoption of a voluntary code of practice and fundamental principles aimed at enhancing visibility, transparency, and education within the digital identity ecosystem in New Zealand. As the ecosystem matures and stakeholders gain insights, it is recommended that the voluntary code of practice transitions into a mandatory requirement for service providers. To reinforce compliance, the independent regulatory body should be empowered with enhanced enforcement capabilities, including the authority to impose penalties for non-compliance. In addition to its current roles of education, reporting, and monitoring, these expanded powers will play a pivotal role in promoting ethical behaviours and fostering increased transparency in the ecosystem

3) Consideration of additional legal powers to give effect to individual ‘agency’

People should have the legal right and freedom to have agency over the data about them and if, how and where it is shared.