City of Toronto

Digital Infrastructure Strategic Framework

Technology Services Division

DRAFT v.10

February 2022

:

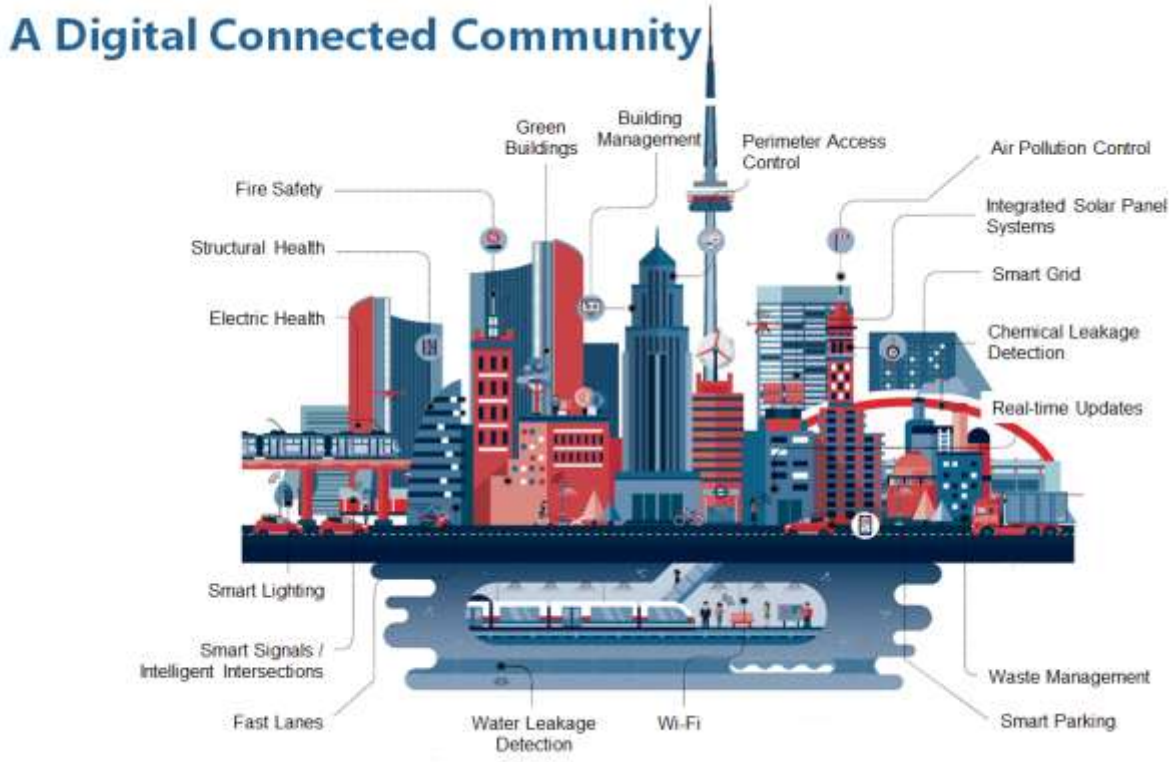
Table of Contents

1. Introduction: A Digital Infrastructure Strategic Framework for Toronto

Toronto: A Digital Connected Community

The use of data and technology provides incredible opportunities – to work in new ways, personalise City services, inform policy and program decisions, and collaborate across silos, thereby addressing societal issues such as housing inequity and climate change. Data and technology can also shape the way many City Council priorities — such as equity, affordable housing, financial sustainability and accessible transportation - can be achieved. However, data and technology are also transforming expectations of public services, and come with challenges — around privacy, accountability, security, protecting digital rights, and social exclusion.

A Digital Connected Community is one where digital infrastructure - defined as technology and data assets that create, exchange or use data or information as a part of their operation - is increasingly used to deliver services, perform data-driven asset management, help manage public resources efficiently, encourage civic engagement, and inform decision-making. In Toronto's journey to becoming a Digital Connected Community, it is important that people can trust digital public services, and feel comfortable and safe when using public digital infrastructure. It is also important that decision making around the use of digital infrastructure, both by the City of Toronto and private actors, include consideration of non-technical alternatives and public buy-in.



1.1. The Digital Infrastructure Strategic Framework

The Digital Infrastructure Strategic Framework (DISF) is a response to the range of opportunities and challenges associated with the use of digital infrastructure, and sets out the overarching vision for Toronto as a Digital Connected Community. The benefits of digital infrastructure will only be realized when they are applied to the right problems and deployed and operated in responsible ways. Objectives, aspirations and values associated with the use of digital infrastructure must therefore be clearly defined and well understood. The Framework aims to clearly define objectives, aspirations and values associated with the use of digital infrastructure and guide Toronto in a direction where:

- Digital infrastructure is used to create and sustain equity, inclusion, accessibility, and human rights in its operations and outcomes
- Digital Infrastructure enables high quality, resilient and innovative public services, and supports the use of data and evidence in decision-making
- Digital Infrastructure is leveraged to create a society that supports equitable and inclusive benefits whether for social, community, health, economic or environmental prosperity
- Privacy and security are at the core of our digital infrastructure, and where residents feel safe and secure online when accessing the City services, systems, and products and services they interact with or choose to use
- Decisions about digital infrastructure are made democratically, in a way that is ethical, accountable, transparent and subject to oversight, and
- The City has full control over its ability to develop, select, maintain and use its digital infrastructure to deliver public services and advance the public interest

The DISF has been developed as a tool to enhance transparency, accountability and consistency of decision-making, while strengthening the flexibility, safety and efficiency of the City's digital infrastructure. In this way, the Framework plays the following key inter-related functions:

1.1.1. Statement of Vision and Aspirations

The *Digital Infrastructure Strategic Framework* is the primary forum for the expression of Toronto's vision and aspirations for digital infrastructure. This vision is expressed through related Principles, Strategic Priorities, and Objectives. This Framework will be used to guide decision-making and uphold the City's values in the digital realm.

1.1.2. Centralized Digital Infrastructure Policy

While a number of policies, strategies and processes within this decision-making framework already exist, further guidance on emerging issues is needed as the use of digital infrastructure increases. As technology changes and new policies, standards and processes related to this infrastructure are developed, they will be housed in a centralized space: the *Digital Infrastructure Strategic Framework*. The administration and accountabilities of underlying DISF components that have an established policy framework - for example, purchasing, privacy, information management, security, data for equity - will continue unchanged.

1.1.3. Framework for consistent decision-making

The DISF is a tool to help guide day-to-day as well as long-term decisions related to the City's digital infrastructure. A central objective of the DISF is to ensure that decisions related to digital infrastructure support corporate objectives and are not made in isolation. The design or procurement of all digital infrastructure at the City should be in compliance with the Principles and related Strategic Priorities within the DISF, as well as other relevant policies, as appropriate.

Audience

The DISF has been written for several audiences:

City staff: The design or procurement of all City digital infrastructure must be guided by the Principles and related Strategic Priorities. The Connected Community team will work with colleagues across the City to facilitate compliance, and to identify and undertake new initiatives that meet City strategic priorities in alignment with the DISF. The Technology Services Division is responsible for oversight and accountability.

Residents: the DISF provides a clear framework for residents to ask questions about digital infrastructure proposed or deployed in Toronto; establishes enhanced transparency and insight into how their data is used; and sets out a common vision on issues such as equity, inclusion, social and environmental benefit, as it relates to digital infrastructure.

Businesses and Innovators: the DISF sets common standards and expectations for new digital infrastructure initiatives within the City of Toronto.

Defining "Digital Infrastructure"

Digital Infrastructure is defined as: technology and data assets that create, exchange or use data, or information as a part of their operation. Digital Infrastructure includes physical objects and structures, such as cameras, sensors and broadband networks, as well as software systems such as mobile applications, websites, open data standards, digital payment, and digital automation. This includes both fixed and mobile devices, such as computers, kiosks, robots, vehicles, and cellphones. It also includes all types of data collected by the City, including administrative data, geospatial data, and personally identifiable information.

Additional definitions are included in Appendix 1.

Organization of the Framework

The Digital Infrastructure Strategic Framework is founded on the following 6 Principles, each with their own chapter:

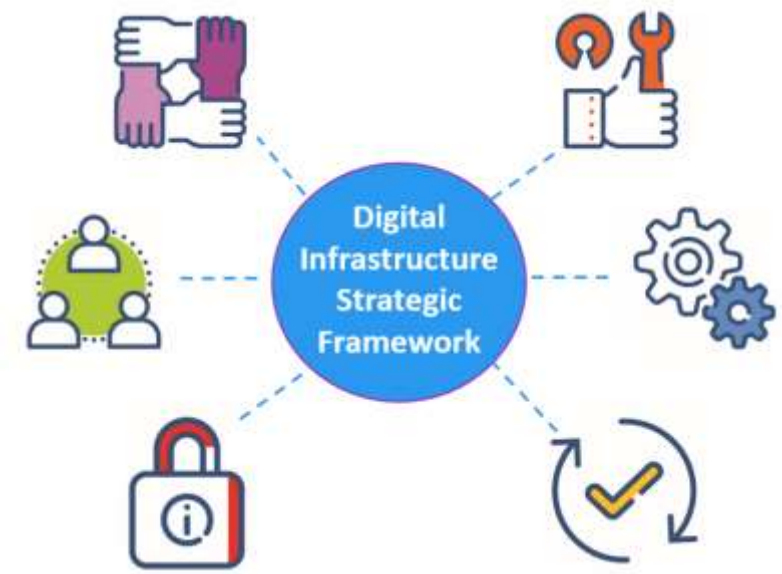
1. Equity and Inclusion
2. A Well-Run City
3. Social, Economic and Environmental Benefits

4. Privacy and Security
5. Democracy and Transparency
6. Digital Autonomy

Each Principle has an accompanying long-term aspirational Vision statement. Themes within the Vision statements are expanded as Strategic Priorities. Consistent with the high-level nature of the Framework, Implementation Considerations are provided for each Strategic Priority. These Implementation Considerations provide guidance for how the Strategic Priorities can be achieved on a case by case basis.

Each Chapter also includes:

- Descriptive text, providing greater context to the Principles, and the different Strategic Priorities identified within each Vision Statement; and
- Informational sidebars, which highlight related initiatives or examples of the DISF in action



Implementation of the Framework

The Digital Infrastructure Strategic Framework is a high level Corporate document that will be used to facilitate and appropriately balance and reconcile a range of diverse objectives associated with the use of digital infrastructure in Toronto. It should be read as a whole to understand its comprehensive and integrative intent as a policy framework for priority setting and decision making. The Framework is more than a set of individual policies, and objectives within the Framework should not be read in isolation or to the exclusion of other relevant objectives. When more than one objective is

relevant, all appropriate objectives are to be considered in each situation. If Toronto is to move closer to the future envisioned in the Framework, all decisions should be evaluated against the objectives within, regardless of scope or budget.

The DISF will be operationalized and implemented on an ongoing basis, as part of the process of business modernization, digital transformation, and asset management. Each project will be evaluated on a case by case basis. As a high-level Framework, policies, standards and or guidelines are needed to provide detailed direction for each strategic priority. In some instances these policies already exist, however additional policies will be needed to enable full implementation of the Framework. For this reason, the Framework will be implemented gradually, overtime, as associated policies, standards and guidelines are developed. In this way, the DISF is envisioned as a "living document", with additional updates also being needed from time to time as the use and nature of technology evolves, as changes take place within the City (for example, via regulatory amendments), as community values shift, or as the DISF itself matures. Any changes to the Framework, other than those that are administrative in nature, must be approved by City Council following a robust process of community and stakeholder engagement.

The Chief Technology Officer is responsible for implementation and oversight of this work, however Division heads are responsible for ensuring the DISF is integrated into divisional business practices. The Chief Technology Office will report out annually with key actions, outcomes, and lessons from implementation of the DISF. Further Monitoring and Evaluation details are included in Chapter 9.

DISF Scope

<u>City of Toronto Digital Infrastructure</u>

The Digital Infrastructure Strategic Framework will be applied to all digital infrastructure projects initiated by the City including:

- Assets owned by the City
- Technology-related initiatives
- Digital Infrastructure operated on behalf of the City
- Associated City of Toronto Policies, Standards and Guidelines
- Existing Digital Infrastructure as it is renewed or replaced over time

<u>Digital Infrastructure not Owned by, or Operated on Behalf of, the City of Toronto</u>

The Digital Infrastructure Strategic Framework will be used to guide and evaluate Digital Infrastructure initiatives that originate from parties other than the City in the Public Realm, where it is determined that those projects have a municipal interest.

For the purposes of the Framework, the Public Realm includes:

- locations regardless of the nature of the ownership where the general public is by right, contract, or custom is invited or permitted to enter
- City streets, sidewalks, parks, transit infrastructure, public squares, etc. as well as private streets, plazas, and ped walkways (e.g. PATH network)

For purpose of DISF, Public Realm does *not* include:

- Commercial, Retail, Industrial, Residential or other property, or to publicly-owned lands that are not under control of the City of Toronto or its agencies (school board lands, Provincially-owned lands etc.).

For the purpose of the DISF, determining municipal interest requires flexibility, but is generally a function of:

- economic, social and environmental well-being of the City;
- health, safety and well-being of persons; and
- protection of persons and property.

2. Principle: Equity and Inclusion

Vision: Digital infrastructure will be used to create and sustain equity, inclusion, accessibility, and human rights in its operations and outcomes. Digital infrastructure will be flexible, adaptable and human-centred, responding to the needs of all Torontonians, including Indigenous, Black, equity-deserving groups, and those with accessibility needs.

This principle describes how the City of Toronto will ensure that people can enjoy their rights and freedoms, feel safe and secure when accessing digital City services (apps, web pages, bill payments, reservations, online permits etc.), and have equitable access to digital City services. All residents and visitors are entitled to respect and fairness online, benefitting from digital services and opportunities without discrimination. This principle reflects the City's motto "Diversity, Our Strength" in the development and use of digital infrastructure.

Equity in the context of digital infrastructure is vital: access to digital tools and services is directly linked to life opportunities, well-being and freedom. The benefits and burdens of the digitized world have not been equally distributed and particular communities continue to experience disproportionate barriers to access and participation which has led to a digital divide. In addition, digital technologies and data are not neutral and have historically had harmful impacts on some communities. Achieving equity in the digital realm requires intentional strategies and investments to reduce and eliminate barriers to access of services and technology. Digital equity also requires an understanding of barriers (i.e. algorithm biases) facing Indigenous, Black and equity deserving communities including those with accessibility needs and strategies to ensure that they are able to trust, participate and fully leverage the benefits of online digital services and technology.

2.1. Strategic Priority: Digital Inclusion and Human Rights

Objective

Digital Infrastructure in the City of Toronto fosters inclusion, and is free from systemic barriers, bias, and discrimination.

Overview

Identifying and removing systemic barriers to the full participation of diverse communities in the digital realm is key to creating equitable access to services and programs for residents and visitors. This need was emphasized even more so by the COVID-19 pandemic. Under the Ontario Human Rights Code, every person has a right to equal treatment in the provision of services and facilities, occupation of accommodation, contracts and in employment. In keeping with these core foundations, the City will strive to design digital infrastructure using an equity lens with the goal of

fostering inclusion and addressing and removing systemic barriers, bias, discrimination and existing inequities.

Emerging Issues

The digital divide presents very real barriers to the use of digital services by many residents (internet affordability, device access, and digital literacy). Other barriers present additional challenges that must also be considered. For example, some older residents may have low levels of confidence using technology, which can lead to them feeling uncomfortable or overwhelmed in the digital realm.

Collecting sociodemographic data can be incredibly useful to understand and address systemic discrimination and inequities. However, it is important to recognize that some residents, including undocumented individuals, may be hesitant or unwilling to provide this information (or to use digital infrastructure and digital services) for a variety of reasons, including if they are required to provide personal information.

Implementation Considerations

1. Design digital infrastructure using equity as a lens, emphasizing human dignity, human rights, ethical digital service standards, and the avoidance of bias and discrimination
2. Identify and address systemic barriers that can restrict the full participation of Toronto's diverse communities in the digital realm
3. Support digital inclusion by strengthening residents' ability and confidence to utilize digital services through initiatives which improve digital literacy, awareness and skills.
4. Engage, educate and train staff - and the broader public - on the value of collecting socio-demographic/ personal information in a standardized way, where appropriate
5. Collect socio-demographic and disaggregated data to identify, monitor, and address inequities in public services, including digital services

2.2. Strategic Priority: Accessible Digital Infrastructure

Objective

All digital City services, products, and information are fully accessible.

Overview

Toronto is committed to ensuring all people can access all City services, products, and information. This includes providing an accessible digital environment where people can access the City's web-based services, information and communications in a way that meets their individual needs (hearing, visual, physical, cognitive, learning etc.) . The City is committed to the identification, removal and prevention of accessibility barriers, and must incorporate accessibility design criteria when procuring or acquiring goods,

services or facilities, except where it is not practicable to do so. Enabling accessibility and usability are achieved through the combination of a number of factors, and not simply about complying with a policy.

Emerging Issues

As more and more City services are made available in digital formats, it is essential that people are not left behind (for example, by the online environment not being fully accessible). The COVID-19 pandemic has had disproportionate consequences on Indigenous, Black and equity deserving communities including people with disabilities. As the City continues to change course it is essential that efforts are made to ensure people with disabilities receive equitable service delivery and supports.

Implementation Considerations

1. Ensure that all City digital services and infrastructure, including websites and web applications, digital kiosks and apps are fully accessible and usable
2. Through training, guidelines and other similar means, ensure that staff are familiar with and know how to use all available accessibility features that are integrated into enterprise software (closed captioning, hand gestures etc.)
3. Integrate accessibility testing from a diverse range of skills and abilities in any new digital infrastructure initiative
4. Work with community and external partners to develop and integrate accessibility functions into materials and products where this has historically been challenging (maps, geospatial data, dashboards etc.)
5. Research and develop a streamlined process for City employees to access American Sign Language (ASL), Communication Access Real-Time Translation (CART) and other accessibility services and supports to provide equitable access to City employees, residents and visitors with disabilities

2.3. Strategic Priority: Human-Centred Digital Infrastructure

Objective

Digital infrastructure, including digital services, are intuitive and easy to use by everyone.

Overview

For digital services to be successful, their design and user-experience must be driven by a fundamental understanding of user needs. The Toronto Public Service and businesses are users too, and to succeed, digital infrastructure must also respond to their needs. These needs are best determined through a Human-centered approach to design. This approach requires an understanding of people in the full context of their lives, and considers a range of perspectives, from childhood through to old age . It also helps ensure that digital infrastructure is sensitive to the privacy and access rights of people with diverse backgrounds and abilities.

Emerging Issues

To ensure that all residents, businesses, visitors and City staff can navigate Toronto's digital infrastructure with confidence and in a self-determined manner, it is necessary to understand the varied needs and experiences of different people - including underrepresented people and those who do not speak English – and involve them in the design of products and services. This can be achieved through meaningful dialogue and ongoing usability testing (I.E. during discovery, design, implementation and evaluation). This process should also apply to existing digital infrastructure, such as the City's website, to ensure it evolves and is consistent with community expectations.

Implementation Considerations

1. Pursue a human-centred approach to designing, developing, procuring and implementing digital infrastructure and services, based on user needs and preferences identified through useability testing, research and consultation
2. Ensure that end users are involved at all stages, including discovery, design, implementation, and evaluation
3. Ensure that continued access to non-digital public services remains available to people who cannot or choose not to access digital services
4. Ensure people can access digital services in a language they understand and that meets their needs
5. Enable users to access digital public services through different channels, devices and platforms, including the ability to switch between different channels through the user journey
6. Foster a consistent, predictable user-experience for City web-based services that is intuitive, simple, and that responds to and evolves with citizens' digital preferences
7. Ensure residents, businesses and stakeholders have the freedom to use the technologies of their choice, and expect the same level of interoperability, inclusion and opportunity in their digital services

2.4. Strategic Priority: Connectivity and Digital Equity

Objective

Residents and businesses have access to high-speed internet and internet-enabled devices.

Overview

Affordable and reliable internet connectivity is essential for a resident's ability to perform the basic activities of daily living, to meaningfully participate in economic, educational, and cultural activities, to enjoy a better quality of life, and to access online City services.Internet service options for residents and businesses vary throughout the city, both in terms of quality and pricing. Free public Wi-Fi is available at most Civic Centres, some recreation centres, all Toronto Public Libraries, TTC subway stations, on some TTC bus routes.

Emerging Issues

As daily life increasingly requires connectivity, Toronto's residents, visitors and businesses must be able to access and use the internet to its full potential. However, infrastructure gaps and other factors related to the digital divide prevent many from fully benefiting from connectivity. The persistence of access and affordability barriers is an indicator of underlying social equity issues. The City is uniquely positioned to leverage public assets for the provision of affordable internet access, and doing this will require a commitment to the principles of digital equity as a foundation for future prosperity.

Implementation Considerations

1. Implement strategic and operational policies to coordinate, centralize, and administer the deployment of City owned fibre infrastructure;
2. Connect City buildings, facilities, and public spaces through a City owned, high-capacity fibre broadband network ;
3. Collaboration with private Internet Service Providers (ISPs) or community-led initiatives to provide affordable, high-quality internet services to residences and businesses
4. Ensure that Indigenous, Black, equity-deserving groups, and those with accessibility needs have access to affordable high speed internet connectivity and internet-enabled devices
5. Enhance resident and business experiences with digital services by using connected and digital infrastructure
6. Support the expansion of full fibre and prepare for 5G, using public assets to stimulate infrastructure investment

3. Principle: Well-run City

Vision: Digital infrastructure will enable high quality, resilient and innovative public services, and support the use of data and evidence to inform decision-making.

A well-run City depends on evidence-based decisions and new insights to inform recommendations, guide decisions and ultimately enable better outcomes. Introducing more online interaction, paperless services, better access to data, and shared services can help create efficiencies and ensure public resources are better allocated. Resilience will enable the public service - and its digital infrastructure - to survive, adapt, thrive and ensure business continuity in the face of the chronic stresses and acute shocks that may arise. Tangible outcomes for residents, business and visitors can include fewer traffic collisions, enhanced quality-of-life, and a more efficient transportation system, and a government that works in deep collaboration with the people it represents to advance an agenda of fairness and prosperity for everyone.

3.1. Strategic Priority: Digital Transformation

Objective

City services, programs, and processes use Digital Infrastructure, when appropriate, to evolve and transform by understanding and anticipating public needs and expectations.

Overview

Digital transformation is an ongoing process in which manual and legacy systems are enhanced or replaced with more advanced digital ones that typically enable greater efficiency, faster service delivery, new capabilities, and better customer experience. Public health standards, fiscal realities, customer expectations and increased comfort level for digital experiences are driving digital transformation at an unprecedented rate.

Emerging Issues

Digital transformation initiatives can be slow, costly, and sometimes fail to achieve the objectives they are intended to accomplish. Importantly, digital transformation does not in and of itself improve existing processes: without evaluating and refining existing business processes, there is a risk that digital transformation will exacerbate existing issues by adding a digital layer to outdated or inefficient processes.

Implementation Considerations

1. Review and refine existing uses of digital infrastructure and digital services to improve how needs are met
2. Clearly define the need for the proposed use of new digital infrastructure in relation to a municipal service or public interest objective

3. Demonstrate that the proposed use of new digital infrastructure is effective at addressing the defined need for transformation
4. Identify and capitalize on opportunities to review and refine underlying business process(es) during digital transformation
5. Explore the use of agile and iterative methods, such as pilot projects, to test and evaluate digital transformation initiatives
6. Work to increase the proportion of services that are available digitally
7. Ensure that any moves towards digital transformation, service improvement, or efficiencies do not come at the cost of public accessibility and privacy
8. Consider the provision and accessibility of alternative, non-digital service channels as part of all digital transformation initiatives

3.2. Strategic Priority: Data Governance

Objective

High quality data management standards ensure that data is protected, accessible, and useable, and facilitate evidence-based decision-making, organizational efficiencies, and improved service delivery.

Overview

Data can provide deep insight into how the city functions, and cities have an ever-increasing need for accessing data: for developing new policies, managing traffic, zoning and planning, enforcement of regulations and monitoring environmental conditions. Better quality and real-time data can improve urban planning, support local decisions and result in more user-friendly services. Data can also play a transformational role in increasing transparency, empowering communities, transforming products and services, and driving innovation. The more data that is collected, the more important it becomes to direct its use in an ongoing and systematic way. To deliver high-quality, integrated services to residents, businesses, and visitors, data must often be collected, shared, and integrated across multiple agencies for operational use, analysis, and evaluation. This is driven by the availability of smart, secure, reliable, up-to-date, and resilient digital infrastructure.

Emerging Issues

The increase in the use of digital infrastructure is leading to more data being collected than ever before. In order to protect the security and integrity of this data, and maximize the potential value of this data, the City requires a data governance framework that will control how data is collected, used, and shared. Data collection in the public realm by

Implementation Considerations

1. Make better, context-driven use of data across the public service, seeking guidance from subject matter experts as necessary, to enable transformation, improve decision-making and improve liveability
2. Develop robust data governance mechanisms for all data stored on domestic systems as well as in the cloud, including appropriate levels of human oversight when necessary, to ensure data is used in an ethical manner, is managed responsibly through its lifecycle, and prevents the risks of abuse or malicious practices
3. Maintain high quality data standards with complementary metadata so it is clear where the data comes from and how it was collected
4. Periodically review and assess the data it collects to ensure it is relevant, required, and in alignment with the City's policy and equity goals and priorities
5. Identify possibilities for greater data integration, analysis, and performance management as legacy technology systems are upgraded
6. Align data governance and privacy frameworks with those being established by the federal and provincial governments, as appropriate
7. Invest in data infrastructure, and improve data sharing and integration capabilities across City divisions and regional jurisdictions
8. Provide service users with assurance that their data is being used effectively for public benefit, efficiently and securely to deliver high quality public services

3.3. Strategic Priority: Asset Management

Objective

Digital infrastructure assets used by the City of Toronto or operating in the City's public realm are governed by a regulatory framework that protects the public interest.

Overview

The City owns and operates digital infrastructure assets, including information technology assets and infrastructure (such as computers, servers, software, and networks) as well as sensors, data analytics, and internet-connected smart infrastructure for a variety of purposes such as providing services, collecting data, and carrying out essential processes. Deploying smart technology effectively has the potential to further improve the City's understanding of its assets, making it possible to plan more effectively, track variations, and even save money. These assets are governed by corporate and technology asset management policies established in accordance with provincial guidelines and best practices.

At the same time, many privately owned and operated sensors and digital assets, including "Internet of Things" devices exist and operate in the public realm.

Emerging Issues

Existing asset management policies may need to be reviewed and updated to align with emerging types and uses of digital technologies. There is currently limited City regulation of emerging and private digital infrastructure, which may expose the City and Torontonians to risks. The use of sensor technology requires coordination of deployments, greater attention to interoperability (that is, the ability for systems or devices to communicate or exchange information with each other), and a mature process of data governance.

Implementation Considerations

1. Define a clear purpose for installing sensors and use sensor technology to improve asset management, quality of life, and meet environmental targets
2. Centralize the approach to sensing devices, including requirements for review, interoperability, open data, coordination of deployments, and decommissioning of obsolete sensors
3. Institute comprehensive review procedures for sensors that emphasize greater inter-divisional collaboration and sharing of historical and real-time data while ensuring compliance with cybersecurity and privacy policies
4. Review and update information technology and corporate asset management policies to align with emerging information about sensors and other digital infrastructure assets in the public realm

3.4. Strategic Priority: Digital Literacy and Adoption

Objective

The Toronto Public Service has the knowledge, skills, and ability to understand, use, and govern digital technologies effectively.

Overview

Digital literacy is the ability to use information and communication technologies to find, evaluate, create, and communicate information. For most people, a foundational level of digital literacy is critical for social, civic, and economic participation. In the workplace, the ability to use technological tools to process work, solve problems, and understand digital content is increasingly essential. Having a workforce with digital and data literacy skills is also an essential component of digital transformation and digital adoption.

Digital adoption is a change and involves a learning process where individuals accept and use new digital resources in the way that they are intended. Digital transformation cannot succeed without digital adoption.

Emerging Issues

The City of Toronto offers a variety of learning and training opportunities for its employees, including content pertaining to digital literacy such as courses on

cybersecurity and privacy. There is an emerging need for public servants who have additional knowledge and skills related to data and digital infrastructure. This will assist digital adoption, technology standardization and alignment efforts, improve public engagement and the quality of digital transformation efforts, and build digital autonomy.

Implementation Considerations

1. Identify competencies and develop training resources to inform a data and digital literacy strategy to enable greater digital adoption and transformation within the Toronto Public Service
2. Ensure that new digital transformation initiatives are accompanied by appropriate digital literacy training and upskilling
3. Develop policies to support a workplace culture that promotes a healthy and appropriate use of digital technologies and work-life balance
4. Support media literacy and develop capacity to respond to misuse and misrepresentations of City data
5. Foster the digital capacity of City staff to develop or deploy digital solutions in a secure cloud infrastructure for City services

3.5. Strategic Priority: Partnerships and Collaboration

Objective

Digital infrastructure and transformation enables, and is enabled by, partnerships between City divisions, agencies, and corporations, the private sector and community groups, different levels of government, and municipalities across Canada and around the world.

Overview

In the search for new ways to address complex challenges, there is a growing recognition that the City can help drive solutions by collaborating across divisions, agencies and corporations as well as across sectors and regions. A city with engaged and informed residents and business sector will attract greater levels of involvement and investment from other levels of government.

The City is a member of a number of working groups, roundtables, and coalitions engaging with municipal, regional, provincial, and federal government agencies, and regularly engages with the academic, civic, and private sectors.

Emerging Issues

It is important for the City to work across organizational silos, build on existing relationships, and develop new partnerships to tackle policy approaches and coordinate cross-boundary matters. The policy and regulatory landscape for digital technologies and infrastructure is rapidly evolving, which requires ongoing engagement with different levels of government.

Implementation Considerations

1. Establish forums to coordinate the refinement and implementation of policies that pertain to digital infrastructure, including the Digital Infrastructure Plan itself
2. Establish and maintain a forum to coordinate technology leadership and strategy across divisions, agencies, and corporations
3. Collaborate with intergovernmental, regional, and cross-sectoral partners, and Higher Education Institutions to align standards, address digital infrastructure challenges and coordinate cross-boundary matters
4. Coordinate with other municipalities to share lessons, expertise and resources on building and maintaining a common open source digital infrastructure
5. Collaborate with provincial and federal governments to interpret how existing or emerging legal frameworks and regulations will apply to digital infrastructure initiatives
6. Support the development of an interconnected strategy with neighbouring municipalities and other levels of government to bolster resilience to shocks and stresses
7. Engage the local civic tech community and domestic innovators to develop, pilot or test digital solutions

4. Principle: Society, Economy and the Environment

Vision: Digital infrastructure will enhance quality of life for Torontonians, support economic prosperity, and advance environmental sustainability, while also avoiding potential harms that could result from its use.

This principle is focused on leveraging digital infrastructure to support equitable and inclusive benefits whether for social, economic or environmental prosperity. In this process, it is essential that potential harms and negative consequences that can arise through the use of technology are avoided. Examples of such harms include: the exclusion of residents from digital services who may not be able to afford residential internet connection; privacy violations; errors, malfunctions or hacks resulting in data leaks or security breaches; and inaccessible digital services resulting in exclusion or discrimination.

4.1. Strategic Priority: Society

Objective

Digital Infrastructure creates positive outcomes for residents as well as society as a whole, including the creation of healthy and vibrant connected communities.

Overview

Digital Infrastructure can be an enabler of rights and freedoms, allowing people to reach out beyond geographic regions and social structures, creating new possibilities to learn, have fun, interact, work, and express creativity. It is also an essential component of crisis management when our critical systems are under unprecedented pressure (healthcare, social services, communication etc.). However, Digital Infrastructure also has the potential to emphasize many social vulnerabilities and broader inequities. It is therefore essential that digital infrastructure does not harm, but rather contributes positively to individuals and society to the greatest extent possible. Some examples include non-discriminatory access to online services; a balanced work-life for those in a remote working environment; the protection of minors in the digital realm; and the ethical use of algorithms and automated decision-making.

Emerging Issues

Digital Infrastructure is increasingly being integrated into everyday objects, such as wayfinding kiosks, benches, bike share, and playgrounds. These types of digital interactivity have the potential to create newfound interest in everyday interactions, which at a broader scale, can lead to new types of creative expression, social interaction, and animation of the public realm. However, all uses of digital infrastructure must be secure, resilient, and operate in a way that protects people's privacy.

Implementation Considerations

1. Use digital infrastructure to modernize services, and improve convenience for residents and businesses,
2. Support community partners to help protect and empower everyone, especially children, youth, and seniors, from malicious cyber activity such as cyber bullying, cybercrime, online hate, mobbing or grooming
3. Support a workplace culture in the Toronto Public Service that promotes a healthy and appropriate use of digital technologies and work-life balance
4. Pursue inclusive and equitable opportunities for digital infrastructure initiatives through community benefits initiatives such as the City's Social Procurement Program, which aims to create jobs, increase supply chain diversity and drive economic growth
5. Broaden the range of vendors tendering to supply digital services, including more small and medium sized enterprises and diverse suppliers from Indigenous, Black and other equity-deserving communities.
6. Support social interaction, creativity and artistic expression through the use of digital infrastructure, including interactive digital media and free public Wi-Fi
7. Give consideration to possible unintended consequences of the use of digital infrastructure prior to its adoption and deployment
8. Develop mitigation strategies to eliminate any unintended negative consequences that may arise from the use of digital infrastructure

4.2. Strategic Priority: The Economy

Objective

Digital Infrastructure helps create opportunities for economic growth and prosperity.

Overview

Digital infrastructure has the potential to bring additional prosperity to Toronto's economy, allowing entrepreneurs to innovate, set up and grow their businesses, and create employment opportunities. The continued success of Toronto's tech, creative and innovative sectors is vital to sustaining our economy, while safeguarding social and environmental wellbeing.

Emerging Issues

Digital Infrastructure has the capacity to disrupt markets and revolutionise industries. The City has a role to play in considering and proactively addressing the potential impacts of disruption caused by digital infrastructure on the local economy.

Implementation Considerations

1. Support domestic business to adapt and be successful in the digital economy, and the City's digital transformation process, including the provision of targeted outreach and education about procurement processes for digital infrastructure
2. Consider the role that digital infrastructure can play in creating local jobs and attracting investment
3. Stimulate innovation through the provision of secure and affordable spaces for testing and experimenting with digital infrastructure (i.e. innovation zones)
4. Collaborate with regional partners, cross-industry partners, and Higher Education Institutions to build capacity and skills, secure investment and research partnerships
5. Set open calls to the tech sector to help solve City challenges in a manner that is ethical and responsible
6. Provide opportunities for domestic technology companies to showcase their technologies (for example through demo days, roundtables, or forums)

4.3. Strategic Priority: The Environment

Objective

Digital Infrastructure helps the City meet climate change targets, and avoid harmful environmental impacts.

Overview

Climate change is a defining challenge of our time. Digital Infrastructure has the potential to significantly contribute to the achievement of emissions reduction goals, and help in the transition to a climate-neutral, circular and more resilient economy. However, digital infrastructure also has the potential to result in harmful environmental impacts. For example, data centres consume substantially more energy than standard office spaces. There is a need to critically examine the resulting impact of greenhouse gas emissions and high intensity use of fossil fuel sourced energy, and the accumulation of obsolete hardware.

Emerging Issues

Decisions related to new digital infrastructure initiatives – including sustainable procurements - need to consider the environmental impact through their lifecycle: will products be repurposed, reused, or recycled, or will they end up in landfill? Will any additional waste be generated? And does the Digital Infrastructure initiative support the efficient use of City resources?

Implementation Considerations

1. Refer to Toronto's climate action strategy - TransformTO - and other initiatives such as the CIO Strategy Council Sustainable IT Pledge - for guidance on how to reduce local greenhouse gas emissions and improve our health, grow our

economy, and improve social equity.

2. Measure, track and report the energy use and environmental impacts of digital infrastructure throughout its full lifecycle
3. Pursue digital infrastructure that is sustainable, such as including renewable energy and recovery of waste heat from digital infrastructure, having a small environmental footprint, and higher energy and material efficiency
4. Extend the service life of devices and equipment through sharing, reusing, repairing, refurbishing and recycling materials and products
5. Identify opportunities to implement circular procurements in digital infrastructure initiatives using the City's Circular Economy Procurement Implementation Plan and Framework
6. Use digital infrastructure to raise community awareness of key environmental issues in order to generate greater commitment to climate change targets

5. Principle: Privacy and Security

Vision: Toronto will uphold human dignity, autonomy and safety by limiting the collection of personal information, implementing safeguards that uphold privacy rights, and protecting digital infrastructure from misuse, hacks, theft or breaches.

Many public services are now deeply reliant on digital infrastructure. The ensuing interconnectedness between City and external systems and data places greater focus on privacy, integrity, safety, security and resilience. This increasing reliance on digital infrastructure brings with it an increased potential for vulnerabilities that could lead to cybersecurity attack, breach, failure, or disruption. Toronto's digital infrastructure requires a "by-design" approach (Privacy-, Security-, and Access- by-Design[1]) to ensure that the benefits created are not overshadowed by the privacy and security risks that may be created.

- Privacy-by-Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.
- Security-by-Design advances the view that properly implemented security processes and technology can enable and protect activities and assets of both people and enterprises.

In recognition that legislation is sometimes slow to keep pace with emerging technology trends, a continual process of review is needed to ensure policies and standards remain current. This will ultimately help maintain the integrity of the City's information, so that it is open, trustworthy, and accessible. Adhering to well-established best practices can also support privacy and security objectives. Examples include the Privacy Protection Principles adopted by the Office of the Privacy Commissioner of Canada.

5.1. Strategic Priority: Consent, Authorized Collection and Use of Information

Objective

Residents are informed when information about them is collected or used for a municipal purpose or by municipally authorized entities operating in the public realm.

Overview

The City is legally authorized to collect, use or disclose personal information as long as it provides an explicitly specified and legitimate purpose, and informs individuals through a "Notice of Collection" statement.

[1] See Appendix 2 for additional information about these approaches

Private sector organizations are required to obtain meaningful consent for the collection, use and disclosure of personal information.

Emerging Issues

Residents are increasingly subject to data collection by the City as well as by privately owned and operated digital infrastructure in the public realm. This presents a number of privacy and security risks. Opportunities to solve civic problems through data sharing also present challenges related to consent and use of data.

Implementation Considerations

1. Ensure that residents are informed when data is collected by the City, and what safeguards are in place to protect their confidentiality and data
2. Ensure that data collection notices explicitly state which divisions and agencies will have access to data
3. Establish expectations, standards and processes regarding authorized collection and use of information for the City, including in scenarios which rely on "implied consent"
4. Ensure that City vendors, businesses and private sector entities are aware of and in compliance with meaningful consent guidelines under PIPEDA.
5. Carry out education campaigns to enhance awareness of the responsibilities of public sector and private sector entities regarding the collection and use of personal information.
6. Ensure that digital infrastructure does not knowingly collect youth data without verifiable parental consent

5.2. Strategic Priority: Privacy

Objective

Privacy risks presented by the use of digital infrastructure are identified, mitigated and clearly communicated.

Overview

Privacy plays a key role in a free, democratic society and is an essential element in maintaining public trust in government. Protecting the information of Toronto's residents, businesses and visitors and maintaining their trust in doing so is key to protecting dignity and autonomy. The City has well-established guidelines to protect personal information collected by the City, while federal law governs information collected by private entities. The City also includes clauses relating to the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) in contracts with suppliers.

Emerging Issues

New types and forms of digital infrastructure implemented by both the City and by private entities can lead to increased concerns about privacy, particularly by members of the

public. Privacy policies and procedures must be updated and strengthened to maintain trust and confidence in digital services.

Implementation Considerations

1. Design and procure all digital infrastructure with Privacy-by-Design principles incorporated
2. Minimize the collection of personal information, and allow individuals to opt-out of automated systems of data collection
3. Review existing privacy policies and procedures to detect, assess, manage, mitigate, and respond to risks presented by digital infrastructure
4. Establish and publicly communicate standards for privacy risk assessment and mitigation
5. Ensure that Torontonians know and understand their privacy rights and data subject rights, and can better control the use of their information
6. Establish and publicly communicate standards for de-identifying or anonymizing personal data collected in the public realm
7. Prohibit data collected within the public realm from being used for advertising purposes without express positive consent
8. Mandate compliance with MFIPPA when contracting private sector organizations to carry out activities that involve the collection, use or disclosure of personal information
9. Strengthen the culture of 'privacy awareness' within the Toronto Public Service, ensuring staff are aware of privacy policies, procedures and responsibilities
10. Implement mechanisms to proactively address concerns about the potential misuse of data by fulfilling individuals' rights to access, review and correct their data

5.3. Strategic Priority: Data Residency in Canada

Objective

Data residency requirements are applied on new digital infrastructure initiatives, where appropriate, to enhance privacy and security.

Overview

As more City services are made available online and information is stored digitally, cloud-based solutions are becoming more frequent. Many cloud-based solutions are located outside of Canadian borders, but cloud service providers are increasingly providing options to store data in Canada as well.

Emerging Issues

If data is stored, in transit, or in use outside of Canada, the City may not be able to apply Canadian laws and regulations that protect it from being improperly used. Data residency requirements can help ensure that public data will remain subject to Canadian privacy and data protection regulations, and that Canadian regulations will govern any

disputes with cloud-based service providers. However, data residency requirements may also limit the ability of the City to engage some vendors and rapidly modernize.

Implementation Considerations

1. Establish a clear framework for determining when and how to apply data residency requirements
2. Ensure that the design, development, and procurement of digital infrastructure considers the question of data residency at the outset
3. Ensure that options for cloud-based solutions consider service providers based in, or with facilities located in, Canada
4. Ensure that City data, including personal information and personal health information, is stored within Canada
5. Ensure that agencies, boards and commissions and private sector vendors comply with City data residency guidelines for personal information

5.4. Strategic Priority: Cybersecurity

Objective

Cybersecurity risks presented by the use of digital infrastructure are identified and mitigated, building cyber-resilience and trust in the protection of data and digital assets.

Overview

Cybersecurity is the ongoing practice of ensuring the City's digital infrastructure, including both technology and information assets, is adequately protected from threats, vulnerabilities, and risks. The possibility of cyberattack must be anticipated, assessed, and mitigated by the City proactively and on a regularly scheduled basis. This is essential to deliver quality and secure interactions between components within the City's digital realm (people, process and technology).

Cyber resilience is key to operational resilience and business continuity, as well as the City's capacity to grow and flourish as we adapt to the increasing move to digital transformation. It ensures that the City can continue delivering services in the event of a cyber incident. Efforts to build cyber resilience are critical to both surviving and even thriving in the face of cyberattacks or physical disasters.

Emerging Issues

The City of Toronto is faced with a rising incidence and severity of cybersecurity risks and threats. Data protection and cybersecurity policies and procedures must be continually updated and strengthened to maintain trust, and respond to the rapidly changing nature of technology.

Implementation Considerations

1. Ensure security-by-design principles are used to design and procure all digital infrastructure
2. Design, develop, operate, maintain, and manage digital infrastructure in alignment with the City's Corporate Cyber Security Policy
3. Embed authentication processes to limit fraud and cybercrime
4. Continuously detect, assess, manage, and mitigate cybersecurity risks emerging from evolving digital infrastructure in order to foster trust in digital services and confidence in local government
5. Protect the data integrity and security of all data collected by the City of Toronto
6. Ensure appropriate auditing, logging, monitoring, and access control are built into all aspects of digital infrastructure
7. Establish and maintain the secure configuration of internet-connected smart infrastructure, including sensors, through such means as device hardening
8. Ensure encryption of any data that contains personal information whether in transit, at rest (i.e. in storage), or in use
9. Strengthen a culture of cybersecurity awareness within the Toronto Public Service, ensuring staff are aware of appropriate policies, procedures and responsibilities

5.5. Strategic Priority: Digital Identity and Access

Objective

Digital identity solutions enable digital inclusion and improve user experience while ensuring privacy, security, and democratic control.

Overview

Digital identity is a fundamental and critical component of cybersecurity that manages user identities and their accesses within an organization. A Digital identity program can:

- help identify risks within programs, processes and projects
- validate the secure usage of City services, assets, and business applications, and
- limit unauthorized access and data breaches within the City.

The federal and provincial governments are also in the process of developing their digital identity programs.

Emerging Issues

Digital identity solutions may increase the risk of digital exclusion, undue surveillance, and reliance on vendors or third parties.

The City's digital identity program should be compatible with those that are being developed by other levels of government.

Implementation Considerations

1. Promote an understanding of digital identity within the City
2. Carry out public engagement and consultation to understand if and how digital identity solutions meet resident needs, and to build trust
3. Identify a framework to evaluate and monitor the privacy and security impacts of utilizing digital identity
4. Ensure digital identity requirements address specific business needs to achieve an intuitive, convenient and seamless user experience
5. Implement ongoing compliance and auditing requirements for all digital identity initiatives

5.6. Strategic Priority: Surveillance

Objective

Residents are protected from undue surveillance and the risks of intrusion and loss of privacy that may be presented by the use of digital infrastructure.

Overview

The City uses traditional surveillance technology, such as CCTV cameras, for a variety of security and safety purposes. CCTV cameras are installed on some building interiors, particularly where large numbers of people assemble; and on building exteriors. When the City collects personal information in this manner, it must tell you how it intends to use the information and provide you with the contact information of someone who can answer questions you might have. Typically this notice occurs through signage that is posted in a clear and obvious location.

Emerging Issues

The increasing use of sensors and digital infrastructure in the public realm, both by the City as well as private entities, leads to a greater risk of surveillance. It is increasingly possible to track behaviour or movement without the knowledge or consent of individuals.

Implementation Considerations

1. Review the risks of surveillance presented by the emerging use of digital infrastructure by the City and by private entities in the public realm
2. Examine and update policies and procedures regarding surveillance
3. Ensure digital infrastructure is developed and governed with guardrails to ensure lawful authority, public safety and respect for privacy

6. Principle: Democracy and Transparency

Vision: Decisions about Digital Infrastructure will be made democratically, in a way that is ethical, accountable, transparent and subject to oversight. Torontonians will be provided with understandable, timely, and accurate information about the technologies in their city, and opportunities to shape the digital domain.

As the closest democratic institution to the people, cities have an important role to play in building trust in digital services and infrastructure that supports our community. This can be done in a variety of ways, including by ensuring that human rights principles of privacy, freedom of expression, and democratic engagement, are incorporated "by design" into the City's digital infrastructure. Approaches such as Access-by-Design [2] and open government advance the view that government-held information should be made available to the public, and that any exceptions should be limited and specific. Access to information enables the public to question the actions of their government and participate meaningfully in policy decisions. Transparency also helps to create a culture of accountability, which in turn can build trust and confidence in digital services.

6.1. Strategic Priority: Public & Stakeholder Consultation and Participation

Objective

Residents and stakeholders have opportunities to participate in the development and design of digital services and digital infrastructure initiatives with the City through open and transparent processes.

Overview

Ensuring Toronto's continued growth as an ethical connected community is a collective responsibility. For people to feel confident that digital public services are reliable and can be trusted, the City must engage fully with all sectors and the general public to ensure their interests are considered. And just like how public consultation is an important step in building out the City's physical infrastructure, so is it necessary for development of the City's digital infrastructure: residents should have the opportunity to help shape the digital realm and share their ideas and content with others. This also includes the involvement of persons who feel anxious about using technology, or find it difficult to keep up with the rapid pace of technological development.

Emerging Issues

The lack of public involvement in decisions regarding digital infrastructure reduces public trust. Decisions around the acquisition and deployment of new digital infrastructure, or sustainment models for existing infrastructure, must take an increasing

[2] See Appendix 2 for additional information about the Access-by-Design approach

number of factors into account: convenience, accessibility, useability, privacy, security, environmental impact, and cost. Stakeholders and members of the public should also be involved in this process, particularly when decision-making results in new technology directions for the City, or when substantial costs can be expected.

Implementation Considerations

1. Promote community awareness of digital infrastructure issues and decisions, through use of clear, understandable language and employing innovative processes to inform the public
2. Establish engagement mechanisms, such as program advisory bodies, to ensure residents and stakeholders are engaged in the decision-making process in development of the City's digital infrastructure
3. Set standards for Indigenous and equity-deserving representation for any program advisory bodies related to the Digital Infrastructure Strategic Framework
4. Create opportunities for residents and stakeholders to provide meaningful input and ongoing feedback to the design, development, and user-experience of digital infrastructure initiatives.
5. Communicate openly with local communities and other groups who might be affected by proposed digital infrastructure initiatives.
6. Through “plain language” communication materials, clearly explain what the digital infrastructure proposal is, what it can do, why it is being considered, and how it will impact them
7. Conduct ongoing engagement and education on digital infrastructure and the DISF itself, so that residents and stakeholders become more familiar with how digital infrastructure relates to them

6.2. Strategic Priority: Open Government, Transparency and Access to Information

Objective

Residents and stakeholders have access to understandable and accurate information about Digital Infrastructure, and insight into associated decision-making processes

Overview

Open Government is about improving the delivery of services, making information more accessible and supporting initiatives that build public trust in government. It is guided by four principles of transparency, participation, accountability, and accessibility. Ongoing Open Government initiatives include providing open access to all Committee and Council agendas, meetings and decisions and the Open Data program.

Open Data is data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed by anyone, anytime and anywhere. When data is made open to the public, new ideas and perspectives unlock the potential for it to be re-used, analyzed, and correlated to help improve the City’s

delivery of public services, engagement with citizens in government decision making, and innovation in our approaches to civic problem solving.

City records, including data and information, are shared in multiple ways with the public, including the City's routine disclosure program, the Toronto Archives, the Open Data Catalogue, and through Freedom of Information Requests.

Emerging Issues

In order to build trust in government, the City will continue to pursue open government initiatives. Access to information is not always simple, fast, intuitive, or user-friendly, and information can remain difficult to access. In addition, Toronto's Open Data initiative requires ongoing support.

As new types of digital infrastructure emerge and are deployed, there are more requests for information regarding them. Greater openness and transparency support the goals of public engagement and democratic control over digital infrastructure.

Implementation Considerations

1. Ensure that residents can easily access and understand information about the City's digital infrastructure: how it operates, and why the decision was made to support its deployment
2. Publish open data about local initiatives and assets to provide insight and transparency into community needs
3. Develop tools to make data processing (management methods, risks, guarantees and rights) accessible and understandable to everyone
4. Commit to the open publication of the criteria for, and rationale behind, any decisions that are made to implement a digital infrastructure initiative that has a direct impact on the lives of residents and clients
5. Publish all internal policies and standards related to digital infrastructure, except in instances where security, privacy or legal matters would be compromised
6. Develop a public registry of digital infrastructure, such as sensors deployed in the public realm; and open source software and hardware projects undertaken by the City

6.3. Strategic Priority: Open Contracting

Objective

Digital Infrastructure procurement processes and related decisions are open and transparent.

Overview

Open contracting is about the increased disclosure of contracting and procurement processes and decisions related to information technology. This includes opening up

information on contracts for both hardware and software. This approach will lead to fundamentally better outcomes for the City such as improving competition, driving efficiency, ensuring value for money, and delivering better quality digital infrastructure. Digital Infrastructure is more likely to serve resident needs if they are involved in the process (useability testing, consultation etc.). Businesses are more likely to bid for tenders if they understand the process. This improves the likelihood of procuring the best digital infrastructure products and services, which in turn helps build public trust and confidence.

Emerging Issues

Open contracting for digital infrastructure requires the inclusive and meaningful participation of the public and a wide-range of stakeholders. This participation includes building effective mechanisms for engagement, ongoing feedback, and continual process improvement.

Implementation Considerations

1. Ensure the City's digital infrastructure procurement processes continue to be fair, open and transparent
2. Disclose information related to digital infrastructure procurements including the tendering process and awarding of all digital infrastructure contracts
3. Encourage innovation and data-driven decision making in digital infrastructure procurement to drive more effective, expeditious, inclusive and sustainable solutions
4. Develop education and awareness materials for domestic firms on how to navigate the procurement process for digital infrastructure
5. Conduct ongoing stakeholder engagement to evaluate and refine digital infrastructure procurement processes

6.4. Strategic Priority: Algorithmic Transparency and Responsibility

Objective

Data driven technologies that use algorithms are used in a manner that reduces risk, and leads to more efficient, accurate, consistent and interpretable decisions.

Overview

The use of Artificial Intelligence (AI), Automated Decision Making (ADM) and similar technologies to support actions and decisions are becoming increasingly common. These technologies have the potential to improve efficiency, asset management, and service delivery. However, these technologies are the product of human choices and are therefore prone to human errors, shaped by human biases and directed by human values. This poses concerns for the privacy, rights, dignity and equality of the individuals or communities affected by them. These types of consequences can significantly undermine and damage public trust and confidence in the use of digital infrastructure. It is therefore critical that public services which rely on AI or ADM respect

the same principles of responsibility, transparency, privacy, and security as all other City services. “Responsible AI” is a concept sometimes used to describe the process of considering issues such as fairness, privacy and security within the design of AI technologies.

Emerging Issues

Algorithms based on historic data can sometimes amplify race, class, gender and other inequalities of the past. As well, algorithms trained on datasets with a lack of diversity or representation can impact the accuracy of the systems (e.g. a facial recognition system may be less effective, depending on skin colour of the person). Another emerging issue with the use of Artificial Intelligence is that it may not always be possible to easily explain how the system arrived at its predictions or classifications.

Implementation Considerations

1. Establish a process for the responsible, accountable and human-centred development and use of transparent AI and ADM, including quality assurance measures for the data, and the AI and ADM technologies, before public use
2. Support transparency by developing a public AI registry, providing understandable and up-to-date information about how AI is used by the City, and how residents may interact with AI
3. Ensure that safeguards are in place to prevent, detect and remedy unlawful discrimination through the use of AI and ADM systems.
4. Restrict the use of systems that for which discrimination cannot be mitigated.
5. Establish data governance mechanisms and ensure appropriate oversight over AI and ADM systems used by the City
6. Integrate the ability to override automated decisions that are inconsistent with the public good

7. Principle: Digital Autonomy

Vision: **The City will maintain control in the selection, use and design of its digital infrastructure, so that it - and its residents - can act with autonomy and in a self-determined manner within the digital realm.**

Digital Autonomy refers to the City's ability to develop, maintain and control the selection, use and design of its digital infrastructure. Examples of digital autonomy include:

- ensuring digital infrastructure is "unlocked" so that the City can repurpose it according to needs. This could include adding new features, or replacing it, without being limited by contractual arrangements (sometimes referred to as "Vendor lock-in")
- having the ability to repair, modify and maintain public digital infrastructure assets, rather than this work only being permitted by manufacturers or prescribed vendors
- enabling interoperability between digital infrastructure, including infrastructure developed by different manufactures, as opposed to these infrastructures being incompatible
- being in full control across the life-cycle spectrum of digital infrastructure, whether it be product design and interface (eg the 'look and feel' of a product), the product outputs or artifacts (eg ownership of data), or product maintenance and management (eg having in-house skills to conduct repairs rather than relying on a vendor)
- individuals being able to access and exert some control over the personal information about them that is held by the City

7.1. Strategic Priority: Open Source

Objective

Open source technologies and solutions are considered and integrated into digital infrastructure that is developed or procured by the City.

Overview

Open-source software refers to all software that can be used, modified and shared (with or without modifications) by any person, and published or distributed under an open licence. Open Source itself is a type of licensing agreement that allows users to freely modify a work (I.E. software code), use this work in new ways, integrate the work into a larger project, or derive a new work based on the original. Open Source Software is integral to digital autonomy as it contributes to interoperability and reusability of solutions; contributes to the avoidance of vendor lock-in (i.e. promotes independence from specific vendors); and promotes collaboration and sharing of solutions across public institutions. Public access to source code is a key component of Open Source Software, which aligns with the Transparency and Democracy principle.

Emerging Issues

There is an increasing reliance on proprietary digital solutions, which can limit interoperability, digital autonomy, and transparency. Considering open source solutions can expand the range of options available to the City, but also requires in-house staff with specialized expertise.

Implementation Considerations

1. Ensure that Open Source solutions are considered in the design and procurement of digital infrastructure initiatives, where appropriate, while promoting free competition in terms of software and hardware purchases
2. Ensure that all code or technological material developed by or for the City are under open licenses and published, where appropriate
3. Use Open Sources licensing to promote the reuse of technological solutions developed by or for the City, including sharing with other public institutions
4. Promote the use of open-source formats for data collection, processing and sharing
5. Encourage the integration of well-established open source software tools in in-house development, where appropriate

7.2. Strategic Priority: Intellectual Property

Objective

The City and public benefit when value is generated from the creation of intellectual property made possible through use of City digital infrastructure and property.

Overview

The development and use of digital infrastructure can help generate valuable intangible assets such as data and code, which can be captured through intellectual property clauses in contracts and other agreements. The City includes clauses relating to intellectual property in City contracts.

Emerging Issues

While the City directly creates or otherwise enables the creation of a range of intangible assets, it can be challenging to capture this value and ensure that it leads to the creation of public benefit.

Implementation Considerations

1. Integrate intellectual property rights clauses into the procurement process for digital infrastructure, where appropriate
2. Seek to ensure that public benefit accrues from Intellectual Property when value is generated by the City or enhanced through partnerships with the City or its residents, when using City digital infrastructure assets.

7.3. Strategic Priority: Open Standards and Interoperability

Objective

Open standards and Application Programming Interfaces (APIs) enable interoperability and encourage data sharing and collaboration between City divisions and external innovators.

Overview

Open standards refer to file formats, protocols and application interfaces that can be implemented by everyone (in open source and proprietary software alike): specifications are available at no cost, and their development and standardization is open and transparent[3]. The use of open standards promotes interoperability and compatible integration between multiple information systems, and are therefore an integral element of digital autonomy. Interoperability is the capacity of different information systems - which could come from different vendors or providers - to work together and share information without technical or legal boundaries. Interoperability is an important element of digital autonomy as it allows for data to be accessible by different systems (also referred to as portability), as opposed to being limited or restricted by proprietary technology.

Emerging Issues

The use of open standards and APIs can advance interoperability considerably. In the longer term, open standards will also facilitate data sharing and collaboration.

Implementation Considerations

1. Ensure that digital infrastructure works and communicates with other technology and systems, and can be easily upgraded, expanded, and that modules can be changed when necessary
2. Establish open standards and APIs for digital infrastructure owned and operated by, or on behalf of, the City
3. Review and identify widely used standards for digital infrastructure to identify ones that are suitable for City use or alignment
4. Enable data exchange to occur between software and data stores / data centres
5. Encourage the use of interoperable digital infrastructure through policies, data, solutions and services

7.4. Strategic Priority: Maintenance and Repair

Objective

The City holds full control over how its Digital infrastructure is maintained and repaired, without barriers in the form of proprietary technologies or legal restrictions.

[3] Open First Whitepaper: Open Standards - Canada.ca

Overview

Maintenance and repair responsibilities and costs are often included in contracts to procure new digital infrastructure and solutions. The repair and maintenance of digital infrastructure can also be impeded by legal protections, software locks, and end user licence agreements. These challenges can hasten the obsolescence of digital infrastructure, leading to increased operational costs and environmental waste.

Maintenance is also linked to building resilience, which is the capacity of individuals, communities, institutions, and systems within a city to survive, adapt, and thrive in the face of the chronic stresses and acute shocks they experience. Stresses and shocks can have both natural (e.g. extreme weather) and human-made causes (eg cyber-attack). All of these events can have significant impacts on residents, the economy, and the environment. In the process of building out digital infrastructure systems, it is necessary to consider what measures are needed to ensure critical support systems can function.

Emerging Issues

Digital infrastructure solutions are becoming harder to fix and maintain, with repairs often requiring specialized tools, difficult-to-obtain parts, or access to proprietary diagnostic software. Integrating the right to repair and reviewing maintenance terms in digital infrastructure solutions and contracts can provide the City with greater control, choice and flexibility around repairs and maintenance, and help meet climate change objectives, but also requires in-house staff with specialized expertise.

Implementation Considerations

1. Integrate Right to Repair requirements into new digital infrastructure solutions, where appropriate
2. Establish maintenance standards for digital infrastructure
3. Consider a 'State of Good Repair' and set appropriate standards for digital infrastructure
4. Identify and maintain acceptable service levels for digital infrastructure, in the event of a major disruption

7.5. Strategic Priority: Democratic Control

Objective

Digital Infrastructure and related initiatives are governed through democratic processes and subject to City oversight.

Overview

To facilitate digital autonomy, and to help achieve the objectives within this Framework, it will be necessary for the City to maintain ownership and control over its digital infrastructure assets. "Control" in this sense is wide-ranging, and will be realized

through a variety of channels such as procurement and licensing agreements; individual rights to access and manage personal information about themselves; the right to repair digital infrastructure; as well as through the digital skill-set of the Toronto Public Service.

Emerging Issues

The increasing growth and reliance on digital infrastructure is leading to significant shifts in traditional power structures. In this context, maintaining control of digital infrastructure assets at a municipal level will ensure the City is better positioned to advance the public interest.

Implementation Considerations

1. Review protocols, standards and contractual or operating agreements to prevent monopolies, barriers to entry, or vendor lock-in
2. Pursue "unlocked" digital infrastructure that can be readily and easily swapped and built upon
3. Establish thresholds to determine when municipal ownership or control of digital infrastructure is warranted
4. Provide a clear rationale when obtaining proprietary digital infrastructure that is controlled - through contractual or agreement or other means - by third parties or vendors
5. Increase residents' control over their personal data collected by the city and how it is shared
6. If a municipal interest in the use of digital infrastructure by a non-City entity has been identified, that use shall be reviewed against the objectives of this Framework and the non-City entity may be required to demonstrate compliance with this Framework
7. Develop guidelines, including minimum application requirements, to regulate the installation of digital infrastructure in the public realm by City and private operators
8. Expand and broaden the range of digital infrastructure service providers and suppliers

8. Monitoring and Performance Measurement

The Framework will be reviewed periodically, but at least once every three to five years, to ensure it maintains currency and relevance.

The fast pace of innovation in the technology sector brings a requirement to ensure that the Principles, Strategic Priorities and Objectives within the Digital Infrastructure Strategic Framework are reviewed regularly for currency and relevance. Course correction will be needed over the life of the Framework and policy changes may also be warranted from time to time. New implementation initiatives may be needed and priorities will require adjustment in response to the varied and changing conditions in the City. Periodic assessment of the Framework will look at the objectives, as well as the outcomes that have been driven by the Framework. These assessments may reveal new emerging strategic priorities that should be addressed through policy initiatives, investment initiatives, or changes to the Framework itself.

Monitoring facilitates our ability to respond to these changes and can improve the quality of decision making. Responsiveness, adaptability and continuous improvement will be enhanced through a commitment to tracking key indicators of social, economic, environmental and fiscal conditions, and by understanding the real changes to our quality of life and their underlying causes. In order to monitor how the DISF is being used across the City, an evaluation matrix will be developed. This matrix will be in accordance with the City's Results-Based Accountability framework that tracks the extent to which DISF guidelines are followed. As part of this matrix, performance measures will be established for each Strategic Priority so that it is possible to measure and demonstrate the impact of the Framework (i.e. How was it used? How well was it done? Who is better off?).

A fair, open and accessible public process for amending, implementing and reviewing this Framework will be achieved by encouraging participation by all segments of the population. Individuals, organizations or other affected parties are welcome to submit comments on the Framework at any time. The evolution of the DISF is intended to be a transparent process. This includes a version history (including a description of consulted parties), with all prior versions of the Framework remaining available for review.

9. Appendix 1: Key Terms and Definitions

Accessible: an adjective, which in the context of the Accessibility for Ontarians with Disabilities Act, means "without Barriers ". The Ontario government creates accessibility standards as laws to make Ontario more accessible

Algorithm: a set of well-defined instructions or rules which produces an output. When we say algorithm, we normally mean an algorithm done by a computer, but the word can also refer to things like bureaucratic rules.

APIs:

Artificial Intelligence: the theory and development of computer systems able to perform tasks that normally require human intelligence. Some examples include visual perception, speech recognition, decision-making, and translation between languages

Barrier: In the Accessibility for Ontarians with Disabilities Act, the term means anything that prevents a person with a disability from fully participating in all aspects of society because of their disability including, but not limited to, physical, architectural, communications, technological barriers, or a policy or practice.

Breach, Security: any incident which results in unauthorized access to a digital infrastructure, regardless of intent

Consent: Free, explicit and informed expression of will by which an individual agrees voluntarily, without pressure, to the collection and processing of data concerning him/her.

Cloud; The Cloud: a set of servers which do what personal computers used to, like run applications and store files. There are many types of clouds, such as "private clouds", where the servers are under the control of one entity, and "public clouds", where access is normally sold on a per-usage basis

Cyber resilience: The ability to prepare for, respond to and recover from cyber attacks

Cybersecurity: the practice of security applied to digital infrastructure. Includes protection of physical digital infrastructure (like literal cables and servers) and non-physical digital infrastructure (like access and storage of data, limiting use of technologies, etc.).

Device Hardening: process to eliminate cyberattack by patching vulnerabilities, turning off non-essential services and enabling security controls such as password management, file permissions and disabling unused network ports

Digital Adoption: The size and scale of usage or uptake of a digital service, compared to a non-digital counterpart. For example, paying bills online versus paying bills in-

person. Can be extended into analogies about people's "digital adoption" and institution's "digital adoption", which typically require further definition

Digital Autonomy: Refers to the City's ability to develop, maintain and control the selection, use and design of its digital infrastructure to deliver public services and advance the public interest, as informed by legislation, community consultation, and the needs of its citizens to adapt to living in the digital realm.

Digital Divide: The disparity within the population regarding access to digital technologies, due either to a lack of equipment and services, or a lack of knowledge and understanding of these technologies.

Digital Equity: equal access and opportunity to digital tools, resources, and services to increase digital knowledge, awareness and skills. This includes the equitable application of digital data, tools, programs and services.

Digital Infrastructure: technology and data assets that create, exchange or use data, or information as a part of their operation. Digital Infrastructure includes physical objects and structures, such as cameras, sensors and broadband networks, as well as software systems such as mobile applications, websites, open data standards digital payment, and digital automation. This includes both fixed and mobile devices, such as computers, kiosks, robots, vehicles, and cellphones. It also includes all types of data collected by the City, including administrative data, geospatial data, and personally identifiable information.

Digital Literacy: Ability to understand and use digital communication technologies, including digital data, in everyday life to achieve personal goals and to expand one's knowledge and abilities.

Digital Rights: the legal and human rights which apply to us all when using digital technologies. These include rights such as freedom of expression, privacy and non-discrimination under protected human rights grounds

Digital Transformation: the intentional reform of organizations and business practices to achieve more value from digital technology.

Discrimination: Any practice or behaviour, whether intentional or not, which has a negative impact on an individual or group protected in Ontario's Human Rights Code (e.g., disability, gender identity, sex, race, sexual orientation, etc.) by excluding, denying benefits or imposing burdens on them.

Equity and Inequity: Equity understands, acknowledges and removes barriers that prevent the participation of any individual or group, making fair treatment, access, opportunity, advancement and outcomes possible for all individuals. In the context of City of Toronto services, inequities refer to unfair and avoidable differences in service access, experiences, impacts and outcomes. Socio-demographic data is a critical tool to

understand who our service users are and if any sociodemographic groups are disadvantaged or require additional supports.

Equity-deserving Groups: Equity-deserving groups refers to communities that face significant collective challenges in participating in society because of barriers to equal access, opportunities and resources due to disadvantage and discrimination, and actively seek social justice and reparation.

While Indigenous people and communities in Toronto face inequities, they are not considered to be an equity-deserving group. Indigenous people are the original inhabitants of what is today Toronto, and have unique status and rights recognized under Section 35 of the Constitution. More than equity, Indigenous communities seek prosperity that is characterized by economic and social well-being, inclusion and self determination, which were eroded through historical and ongoing colonization.

While Black people in Toronto also face inequities and seek equity, they are recognised as unique and separate from other equity-deserving groups. People of African descent who commonly self-identify as Black people have a unique experience of centuries of enslavement in what is now Canada. The time period of legalized enslavement was longer than the period during which Black people have been legally free. The legacy of socio-economic enslavement continues to significantly impact Black communities in Toronto and across Canada through inequities in social and economic outcomes and well-being. As such, Black communities are more appropriately to be considered as freedom-seeking.

Ethical digital service standards: concerns the questions of how developers, manufacturers, authorities and operators should behave in order to minimize the ethical risks that can arise from the use of digital infrastructure in society, either from design, inappropriate application, or misuse.

First Nations: Adopted in the early 1980s, this collective term refers to the original Nations who existed across the territory for thousands of years, and who were colonially referred to as “status and non-status Indians” under the Indian Act, 1876.

Hack, Security: refer to Breach, Security

Hardware: refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners.

Human-centered Design: An approach to understanding people in the full context of their lives in order to design policies, programs, products and services that best meet their needs. Through customer experience research and public engagement, we learn about their needs, goals, pains, and mindsets, generate and test ideas with them and keep them engaged through ongoing feedback

Implied Consent:

Indigenous: a term used internationally to collectively represent the original inhabitants or those naturally existing in a particular place. In this context, "Indigenous" is used to refer to the First Nations, Métis and Inuit.

Intellectual Property: a branch of law which extends the concept of property to intangible creations of the mind. Examples include copyrights, patents, trademarks and trade secrets.

Internet-connected smart infrastructure (also referred to as Internet of Things): Digital Infrastructure such as sensors, devices and wearables, that are connected to the internet and which generate data

Interoperability: the capacity of different information systems - which could come from different providers - to work together and share information without technical or legal restrictions

Legacy system(s): older technology systems, typically using programming languages and physical technologies which are no longer in common use, are less likely to be interoperable, and which can be hard to continue to support.

Metadata:

Open-by-default:

Open Data: Digitally structured information, in machine readable and accessible formats, made available to the public under an open data licence

Personal Information: recorded information about an identifiable individual. This definition comes from provincial public-sector law, which puts restrictions on how governments can collect and use this type of information

Privacy by Design: To build privacy and data protection, into the design specifications and architecture of information and communication systems and technologies at the beginning, in order to facilitate compliance with privacy and data protection principles.

Privacy Breach: The improper or unauthorized creation, collection, use, disclosure, retention or disposition of personal information.

Privacy Impact Assessment (PIA): an in-depth review and analysis of a project, program, technology system, and/or process and is intended to identify and resolve privacy risks throughout the design or redesign of a technology, system, program or service.

Procurement: The acquisition of goods and/or services by any contractual means, including purchase, rental, lease or conditional sale

Publish with Purpose

Racialized: Racialized persons and/or groups can have racial meanings attributed to them in ways that negatively impact their social, political, and economic life.

Right to Repair: a proposed legal idea, which would provide the practical means for electronic equipment owners to repair their devices. There is no inherent right to repair in Ontario nor in most of the world, but when purchasing technology this can sometimes be negotiated.

Reconciliation: Digital Infrastructure will be used to create mutually respectful relationships between Indigenous and non-Indigenous people, including awareness of the past, acknowledgement of and atonement for the harms that have been caused, and actions to change behaviour. Actions taken for Reconciliation will be taken in partnership with Indigenous Peoples, and directly respond to the self-identified needs and directives as set out by Indigenous community members, organizations, and leaders.

Secure Development Lifecycle: process of including security artifacts in the Software Development Lifecycle

Sensors: an electronic device which collects data about the physical world, such as light (e.g. cameras), sound, heat, motion, etc., and transmits it to a computer

Software: programs and other operating information used by a computer.

Socio-demographic data: Socio-demographic data describes personal characteristics and social identity. Characteristics such as age, language, race, First Nations, Inuit, Métis identity, Canadian-born or immigrant, disability, gender, sexual orientation, income and place of residence are all examples of socio-demographic data.

Standards: a document which provides a set of agreed-upon rules, guidelines or characteristics for activities or their results. Technical standards are typically established by governments, by standards development organizations and industry associations

Systemic Barrier: A barrier embedded in the social or administrative structures of an organization, including the physical accessibility of an organization, organizational policies, practices and decision-making processes, or the culture of an organization.

Threat Risk Assessment (TRA): process for identifying the threats to confidentiality, integrity, or availability of Information Technology (IT) assets, assessing current vulnerabilities for each IT assets based on existing or proposed controls, analysing and quantifying the risk levels for the vulnerable IT assets, and providing recommendations to lower the risks to acceptable level.

10. Appendix 2: "By-design" approaches to Privacy, Security, and Access

A "By-design" approach to Privacy, Security, and Access

A "By-design" approach for Privacy, Security, and Access will be taken for all digital infrastructure initiatives. "By design" is an approach where certain objectives or desired outcomes are considered and integrated into all phases of a project, starting with design but including the entire lifecycle. This approach ensures that these objectives are proactively integrated directly into the design of digital infrastructure systems, processes and services by default. This also includes the business processes and practices which support that infrastructure. Other "by-design" approaches may be integrated into digital infrastructure initiatives, as guided by objectives and desired outcomes.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Security by Design advances the view that properly implemented security processes and technology can enable and protect activities and assets of both people and enterprises.

Access by Design advances the view that government-held information should be made available to the public, and that any exceptions should be limited and specific.

The Principles of Privacy-by-Design are:

1. Proactive not Reactive; Preventative not Remedial - Anticipate and prevent privacy invasive events before they occur
2. Privacy as the Default - Automatically apply privacy as a default feature
3. Privacy Embedded into Design - Incorporate privacy as a key feature of the design of digital infrastructure
4. Full-Functionality - Make an effort to accommodate all reasonable and legitimate privacy and security features and functions
5. Full Data Lifecycle Protection - Map the entire lifecycle of data, and protect it from breach at all stages
6. Visibility and Transparency - Allow full access to and independent verification of all technology and business practices which use personal information
7. Respect for User Privacy - Offer users measures such as privacy defaults, consent, and appropriate notice of collection

The principles of Security-by-Design are[4]:

1. Begin with the end in mind. Leverage enterprise architecture methods to guide the proactive implementation of security
2. Implement "Secure by Default" policies, including least privilege, need-to-know, least trust, mandatory access control and separation of duties.
3. Apply Software Security Assurance practices. Use hardware solutions such as Trusted Platform Module.
4. Accommodate all stakeholders. Resolve conflicts to seek win-win.
5. Ensure confidentiality, integrity and availability of all information for all stakeholders.
6. Strengthen security through open standards, well-known processes and external validation.
7. Respect and protect the interests of all information owners. Security must accommodate both individual and enterprise interests.

The Principles of Access-by-Design are:

1. Proactive not reactive - a proactive approach to promote full transparency
2. Access embedded into design - making proactive disclosure the default
3. Openness and Transparency - support the democratic process by ensuring that citizens have the information required to hold government accountable
4. Fosters Collaboration - make data readily available so that it can be used to advance society as a whole
5. Enhances Efficient Government - improve information management practices by providing more streamlined access to public information
6. Makes Access Truly Accessible - requires that public information be easily found, indexed and presented in user-friendly formats
7. Increases Quality of Information - implement quality control and assurance protocols to ensure that information is accurate, reliable, and up-to-date

[4] Privacy and Security by Design: An Enterprise Architecture Approach