City of Edmonton Information Technology Standards for Procurements
For Use In All Procurement That Contain Information Technology Components

These standards provide general information regarding the services provided by the Open City Information Technology (OCT) branch, in the context of implementation projects. These standards are published through consultation with subject matter experts. Respondents who have questions regarding these standards should engage the CPSS contact identified on the Procurement they are engaging in or responding to.

Section A - Standards that Apply to All Procurements

These standards apply, regardless of where the Solution may be hosted.

- The Solution(s) should ideally be based upon open systems architecture standards in which the design and technology follow public, non-proprietary standards and specifications allowing for the ability to integrate with multiple hardware and software providers to support compatibility and interoperability with City systems.

1. Project Management	
Methodology	To deliver technology projects, the Open City & Technology Branch uses the Technology Project Delivery Framework. The framework lives within the City of Edmonton standardised Project Development & Delivery Model (PDDM); it is also enclosed by, and distinct from, the Corporate Business Technology Investment Framework - which is the overarching investment life-cycle determining governance, funding, and benefits realisation. The Technology Project Delivery Framework determines how solutions are delivered. This framework is owned and curated by the Technology Project Management Office, and follows PDDM as well as Project Management Institute (PMI) best-practices. The framework outlines the life-cycle followed by all technology projects, from the hand-off from Technology Planning to closure, and the main stakeholder groups involved in the delivery of technology solutions and their roles & responsibilities.
Project Lifecycle / Gating Process	Within OCT, the Technology PMO strives to match the level of risk for each technology engagement type with a corresponding level of rigor and documentation. The business technology landscape is ever-changing and the framework is continually revised and improved to keep up with the change. To understand the applicable process and deliverables, please refer to the delivery framework overview in conjunction with the responsibility matrix. PMIS Project Online is OCT's Enterprise Project Management (EPM) and Project and Portfolio Management (PPM) solution, used to manage all technology projects (incl. Managed Work Requests) run by OCT for the City of Edmonton. PMIS is the core platform of the Technology PMO, through which we manage and track all information related to our engagements. The solution facilitates Financial Management, Schedule Management, Resource Management, Status Reporting, Portfolio-level reporting, standardisation of Workflows, among many other features.

	Determination of whether a technology initiative should be reported through the PMIS Project Online platform is done during consultations with Technology Investment Governance for new initiatives. Criteria for mandatory inclusion in PMIS: 1. OCT-funded, in whole or partially, through the renewal or growth capital profiles, operating funding, or a combination thereof; or 2. The technology engagement is a Project or Managed Work Request coordinated by an OCT PM. Criteria for when a technology engagement can be considered for inclusion in PMIS: 1. The prime PM is a City of Edmonton resource (i.e. internal staff member or Flextrack/staff augmentation contractor PM); 2. The project sponsor and PM agree to adhere to the PMO framework and constituent rules (i.e., documentation/responsibility matrix, usage of Google folders, keeping PMIS record up to date, biweekly project status reporting, etc.); and 3. The engagement was initiated through the OCT Technology Investment intake process. Implementation of any information technology to City of Edmonton staff normally should utilise the PMO framework and system for the IT-specific components of the Project, even if the primary purpose of your Project is not Information Technology. For all technology implementations following Technology PMO rigor, bi-weekly status reports must be submitted through PMIS.
2. Cyber Security and Risk Management	
Information and Data Management	Information and Data must be created, collected, used, classified, protected, preserved, and disposed of in accordance with applicable legislation, such as the PPA (Protection of Privacy Act) and AITA (Access to Information Act) within Alberta, and PIPEDA nationally and also adhere to corporate policies, standards, processes and procedures. Government records must be preserved in a manner that protects authenticity, accessibility and context throughout the information's lifecycle.
General	Solutions must adhere to industry-standard (or better) security frameworks, procedures and technologies. These frameworks or standards include, but are not limited to: NIST CSF v2; ISO 27001/27002/2700x; CIS Controls; SOC 2; PCI DSS; COBIT; CSA Cloud Control Matrix; etc.) The level of security controls must be reasonable given the risks and information managed by the application, and must be compatible with existing City of Edmonton security infrastructure. Installation, support, development and enhancements of solutions must be performed

	on-site. If this is not possible, remote access will be provided by the City of Edmonton using an existing remote access solution.
Infrastructure	All City-managed computers (server, desktop, laptop) will operate with a client from the CISO's managed detection and response service. Solutions deployed to computing devices should not require Local Administrator privileges to operate. Local connections to the City of Edmonton network must be done with City-managed devices. Direct connection of devices not managed by the Open City and Technology Branch to the City of Edmonton internal corporate network is not permitted. Remote access to the City of Edmonton network is limited to use of City of Edmonton approved and managed access solutions. Multi-factor authentication is required for access to any City computers.
Internal Solutions	Information stored locally on mobile computing devices must be protected by an appropriate data security solution, as determined by the City of Edmonton. Encryption of stored data requires City of Edmonton approval and must include key escrow procedures to ensure encryption keys are available when staff are absent.
External Solutions	Any secure Internet site which the City of Edmonton is required to use as part of a solution must be signed with a valid and trusted certificate. Self-signed certificates are not accepted by the City of Edmonton as either valid or trusted. Any communication over a publicly accessible network that involves the transmission of City of Edmonton information must be encrypted by an industry accepted encryption protocol. Adequacy is subject to City of Edmonton approval.
Enterprise Solutions	Use of enterprise or shared IT solutions, resources, and services to avoid duplication when available, appropriate and/or required by corporate policies, standards, processes, or procedures. This includes leveraging, when reasonable, existing Preferred common City Enterprise solutions listed but not limited to the following : ● Google Gemini is the Generative Artificial Intelligence (AI) Solution. ● AEGIS as the Geospatial Standard for maps, location-based and spatial data ● SMTP Relay as the City's Standard method of email forwarding replacing SPF records.
Desktop Software	The applications detailed here are available on all standard desktop installations at the City of Edmonton. The standard operating system for desktops is Microsoft Windows 11 64 bit.

Office Productivity and Collaboration Software	Users have access to the Google Workspace suite which includes but is not limited to : ● Google Drive, Gmail, Google Calendar ● Google Docs, Google Sheets, Google Slides ● Google Meet, Google Chat Note: Additional Microsoft Office suite of applications are available as complimentary productivity tools on an exceptional basis provided the appropriate business requirements and funding have been approved.
Web Browsers	Latest available and/or supported versions of ● Google Chrome ● Microsoft Edge
Software Fax	A printer-based Fax Service is available.
5. Email & Calendar	
Email & Calendar	Google Email and Google Calendar are the standard email and calendar service offerings. Exchange services are available for application integration use. Archival services are provided to all email services. Filtering of email, for phishing, spam, and other security purposes, is actively performed. Communications via email to the City staff must be done with valid and properly configured mail servers, such as valid SPF and MX records.
6. Open Source	The following standards only apply to respondents proposing to include Open Source Technology as part of their proposal.
Product Roadmap	The City of Edmonton encourages vendors to submit roadmaps for open source products as part of a Procurement response to ensure we have an understanding of how the product's features will be changing over the near future.
Product Support	All Procurement responses that are suggesting the use of an open source product must contain elements that detail how adequate support for this product will be provided. Adequacy is determined by the City of Edmonton.
7. Web-based Applications	The following standards only apply to internal or non-public facing web-based applications or websites.
Accessibility	Must allow all users (including those with visual impairments or physical disabilities) to access the application according to recognised accessibility standards set down by the World Wide Web Consortium (W3C) incorporating WCAG 2.0 conformance.

Encryption	Protects web application with HTTPS, even if it doesn't handle sensitive communications, and ensures that the latest TLS versions are supported and configured.
Browser	Must support the latest available and/or Supported versions of : - Microsoft Edge (Windows) - Google Chrome (Windows, MacOS and Linux)
8. Public Facing Web Applications	The following standards only apply to web applications or websites that are public facing.
Visual Identity, Colors and Fonts	Must be able to follow CoE Visual Identity Standards and CoE Style Guide and Pattern Library.
Encryption	Protects web application with HTTPS, even if it doesn't handle sensitive communications, and ensures that the latest TLS versions are supported and configured.
Accessibility	Must allow all users (including those with visual impairments or physical disabilities) to access the application according to recognised accessibility standards set down by the World Wide Web Consortium (W3C) and incorporating WCAG 2.0 conformance.
Google Analytics	Must be able to embed the Google Analytics to track the visiting traffic details.
Browser	Must support: Any modern standards compliant web browser that is the most current stable channel release: e.g. - Microsoft Edge (Windows) - Google Chrome (Windows, Mac and Linux) - Mozilla Firefox (Windows, Mac and Linux) - Safari (Mac) - JAWS, VoiceOver and other screen readers
Accessibility	Must allow all users (including those with visual impairments or physical disabilities) to access the application according to recognised accessibility standards set down by the World Wide Web Consortium (W3C) incorporating WCAG 2.0 conformance.
Videos	Videos in the application are provided in HTML5 format, which must be supported by the browsers that are specified above.
Audio Clips	Audio clips in the application are provided in mp3 format.

Section B - Standards that Apply to City Hosted Solutions	
These standards apply where the services or servers are to be located at a City of Edmonton datacenter.	
1. Computing Facilities	
General	The City of Edmonton maintains multiple computing facilities. All solutions that are hosted by the City should be capable of being hosted from these facilities and must conform to IEEE standards.
Rack Sizes	All equipment that is to be hosted at a City of Edmonton computing facility must be mountable in a standard 19-inch rack (EIA-310). Devices should be mounted on all 4 posts. The City will have to approve solutions that only offer 2 post mounting options.
Data Centre Network	All devices should have a minimum connectivity of 1000 Base-T. The default connectivity for host devices is 10G Base-SR. Only wired connections are acceptable for servers. Devices should support LACP (Link Aggregation Control Protocol) for creating the links to the data centre fabrics. This is to provide resilience. Other dual connection solutions will be evaluated on a case by case basis by the City. IPv4 must be supported on the device.

Internal Campus Network	Internal wired network connections exist at all city facilities. Any product, device, or application requiring network access, or sending/receiving data across the city's network that does not meet CoE Server, operating system, hardware or software standards requires prior approval on a case by case basis. Wi-Fi may be leveraged for connecting some client devices as part of solutions. All new installations should support WPA3. All solutions must support the Enterprise methods of authentication within the WPA3 suite, and they should have a reasonable method for the distribution of the certificates to the devices for the Enterprise methods of authentication as part of the solution. The City evaluates if exceptions to this can be accepted. Pre-Shared Keys are undesirable in the Enterprise and they do not conform to the Enterprise methods of authentication in the WPA3 suite. Wi-Fi coverage may need to be enhanced. This is determined by the use case. It is desirable that Wi-Fi client devices support Wi-Fi 6E (IEEE 802.11ax) IPv4 must be supported on the device.
Remote Access	Vendor remote access is offered by the City of Edmonton, if required.
2. Data Storage & Backup	
Data Storage	The City of Edmonton maintains a data storage-area network, that is available to all solutions hosted at the City of Edmonton computing facilities. Network File Storage (NFS) and SMB (Server message block) is also available in addition to an NFS/SMB pass-through for communication between Windows and Linux based systems Mirroring between data centres is available, if required, to enable higher availability of systems.
Backups	All production corporate information that is hosted on premise is subject to regular backups. Backups also include off-site storage as part of the City of Edmonton's Disaster Recovery plans. Data that is hosted externally requires a tested recovery strategy and business continuity plan that reflect the business objectives.

3. Telecommunications	
General	Telecommunications services to the City's 400+ sites are provided through a combination of Voice over IP and Analogue Services. Any telecommunications device or application must utilise existing telecommunications infrastructure. The use of analog telephone services requires approval by the City of Edmonton.
Voicemail	Voicemail is provided by a combination of City owned systems devices and contracts with service providers.
Cellular	Cellular to City of Edmonton devices provided through a combination of contracts for service with Telus and Rogers. Any cellular devices or related applications should utilise existing providers.
IoT - Internet of Things	IoT is provided by a combination of City owned network or LoRAWAN systems or approved vendor provided cellular listed above.
4. Database	
Enterprise Environments	The City of Edmonton supports two enterprise class database platforms depending on the Operating System: ● Oracle ● Microsoft SQL Server The use of other enterprise level database environments must be justified on an Exception basis.
Database Development	The City of Edmonton provides limited development support for local and middle tier database applications. Technical support at this level is limited to the provisioning of the database platforms and does not extend to the support of end-user applications developed using these database solutions. Limited "best-effort" application support may be available in certain circumstances.
Data Lifecycle	The City of Edmonton requires the ability to manage application data lifespan with archive and purge options in accordance with the City's data retention policies.
5. Desktop Computing Devices	
Operating Systems	These are the City's primary standard supported desktop and laptop operating systems. ● Windows 11 64 bit ● Google Chrome OS Not all operating systems are available on all classes of devices. Alternative platforms may be available as exceptions.
6. Internal Authentication	
General	Active Directory provides an authoritative source for authentication within the City of Edmonton network, including employees and external affiliates.

Single Sign-On	Internally hosted solutions must have the capability to integrate with industry standard authentication services such as Active Directory LDAP, SAML, OpenID Connect or OAUTH with integration into COE available directory services.
Integration	Internally hosted solutions must be capable of integrating with COE directories or COE Identity Governance and Administrative (IGA) systems for the purpose of account provisioning and deprovisioning, or provide administrative interfaces to directly provision and deprovision digital identity within the solution. On-demand integration with Active Directory, such as for authentication, should not be performed except through a City of Edmonton approved authentication source.

Section C - Standards that Apply to Hosted Solutions

These standards apply where the services or servers are to be located at a location managed by a service provider.

Cyber Security Contractual Requirements	The following requirements do not replace the need to comply with the City's Administrative Directives, Administrative Procedures or other City accepted practices. Definitions - Unless otherwise specified, words used in this directive and its accompanying procedures have the same meaning as defined in either the City Administration Bylaw, Bylaw 16620 or the COE Cyber Security Glossary.
	The City must retain ownership of the Digital Assets, such as information. The City must retain the right to repatriate the Digital Asset. After the repatriation, the Service Provider must securely wipe the Digital Asset, within a timeline that is set by the Asset Owner, and must provide the City with a certificate of destruction. The City must specify the conditions under which the Service Provider is authorized to use the Digital Asset. The City's Digital Asset must be adequately segregated from non-City Assets. The Service Provider, and its sub-providers, must securely operate the Data Centers and all aspects of the technology, such as operational security, encryption, incident detection & response, identity and access management, in compliance to City standards. Industry accepted cyber security practices may be considered. Upon their knowledge of a cyber security incident, the Service Provider must notify the City within 8 hours of a major incident, as defined by the City, and within 24 hours of all other incidents.

Cyber- Security Compliance	The Service Provider must provide the City of Edmonton with an annual independent security audit demonstrating their compliance to industry certifications or attestations, such as : - SOC1 (controls over financial reporting) - SOC2 (controls over security, availability, confidentiality and privacy) - SOC3 (public report of controls over security, availability, confidentiality and privacy) - ISO 27001 (managing information risks) - ISO 27017 (controlling cloud-based information security) - ISO 27018 (protecting personal data) - Cloud Security Alliance (CSA) STAR Attestation - Cloud Security Alliance (CSA) STAR Certification - FedRamp certification - GDPR Compliance OR - if the Service Provider does not have attestations, certifications, or formal compliance evidence as listed above, they must produce adequate detailed Cyber Security Control evidence to the City that is deemed as equivalent or better to the requested security standards, and the Proponent acknowledges that such evidence may be accepted or dismissed as insufficient at the discretion of the City.
Cyber Security - Right to Assess	The Service Provider must allow the City, or its appointed experts, to perform their own cyber security assessments of the Service Provider. - Both City representatives or appointed experts are to provided the same access to information, documents and facilities as required to complete the assessment. - Unless otherwise specified, the City will bear the cost of the cyber security assessment unless the cyber security assessment identifies significant findings that show that the contractual obligations with the Service Provider are not being met.
2. IT Disaster Recovery	
Disaster Recovery Contractual Requirements	All Solutions must include a Disaster Recovery plan specific to the requirements of the business. This applies whether the solution is to be hosted by the City of Edmonton or by a third-party All City of Edmonton solutions are required, as part of the Business Impact Assessment, to define Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) appropriate to the Business need.Recovery Time Capabilities must align to the City of Edmonton's Recovery Time Objectives. This can be demonstrated via disaster recovery testing. Gaps between RTO and RTC must be raised to the CoE in order to address the disparity. The Service Provider’s recovery time capabilities must meet the City’s identified

	recovery time objective. If the application or service is determined to be critical to the City, the Service Provider's applications or services are to be highly available. Unless otherwise agreed, the Service Provider will perform back-ups of City data and these back-ups are to be both immutable and encrypted in transit and at rest. Where agreed with the City, the Service Provider will provide 24/7/365 support. The Service Provider will annually provide evidence to the City of a disaster recovery plan. Due to proprietary reasons, this may limited to a table of contents. The Service Provider will provide evidence to the City that the disaster recovery plan is tested and/or exercised at least annually.
Backups	Unless otherwise agreed, the Service Provider will perform back-ups of City data and these back-ups are to be both immutable and encrypted in transit and at rest.
3. External Authentication	
General	All external solutions must provide application security, including role-based access control ,follow multi-factor authentication (MFA) requirements and support the City's password complexity rules such as minimum length, password expiration and include three out of four criteria (upper case, lower case, numbers and/or symbols)
Single Sign-On	It is desired that externally hosted solutions have the capability to integrate with the City's authentication services. They should rely on existing standard authentication processes, such as SAML, OpenID Connect or OAUTH using standard COE Identity Provider systems.
Integration	It is desired that externally hosted solutions be capable of integrating with COE user digital identity provisioning and deprovisioning processes, either directly or indirectly using COE Identity Providers or COE Identity Governance and Administration (IGA) systems.
4. Application Design & Configuration	
Design	All applications must include a high-level design diagrams showing all associated components and subcomponents
Configuration	The application should allow customisation and/or configuration to maintain City of Edmonton communications design guidelines regarding the visual look and feel of the application. The proponent of the application should describe how the application could be moved to a different platform or functionality transitioned to another application.
5. Integration	
Web Services	The preferred method for accessing City data is secure web-services that use industry-standard protocols and message formats. The functionality of the application should be consumable via web services to enable

	real-time integration, or as near to real-time as is reasonable.
Data	The City's data must be available to other City of Edmonton applications including business intelligence and statistical reporting tools.

Section D - Payment Card Industry (PCI) Compliance

	The City's Infrastructure must be kept Out of Scope for PCI DSS Compliance
	All components of the solution that process, store or transmit payment card (credit/debit) data must be PCI compliant : ● PCI PTS compliance for hardware; and ● PCI PA-DSS compliance for software. Vendors must provide Attestation Of Compliance (AOC) documents confirming the level of PCI compliance and the solution(s) must maintain PCI compliance status throughout the duration of the service.