Acceptable Use of City Technology Resources (AUP)

Standards for City of Calgary Technology Resource Users and City Management

Approved by IMSGC: 2016/05/19

Contents

Purpose

This standard applies to all City of Calgary technology resource users at all levels of the organization which use technology. The City is committed to safe and responsible use of technology resources to protect The City's reputation and ensures responsible use of taxpayer dollars. This policy protects the interests of both The City and its authorized technology resource users including: employees, temporary and seasonal staff, consultants, contractors, volunteers and vendors.

The standards covered within this document are to provide clarity around the responsibilities City technology users have when using City technology resources. Specifically:

- Appropriate use of The City's technology resources for business and personal purposes,
- Monitoring, and
- Responsibility for reporting, following and enforcing the *Acceptable Use of City Technology Resources Policy*.

As the *Acceptable Use of City Technology Resources Policy* (AUP) impacts how City of Calgary technology resource users behave, it is one of several policies within the Corporation's Code of Conduct.

Exemptions to this standard

These standards do not apply to members of City Council and their staff or to Calgary Police Service personnel. Those organizations are responsible for governing their use of technology resources.

Roles and Responsibilities

All employees of The City of Calgary are responsible for managing The City's technology resources in an acceptable manner. The AUP and this standard outline the behaviours and responsibilities employees at all levels of the organization are to follow when using technology resources. Technology resource users include:

- Permanent staff,
- Temporary and seasonal staff,
- Consultants,
- Contractors,
- Volunteers
- Vendors

Information Technology (IT), Law-Corporate Security, and Human Resources (HR) have specific roles and responsibilities for supporting City management in meeting the AUP policy and standards.

Ultimately, supervisors and managers are responsible for ensuring technology resource users are using the technology resources supplied in a way that is appropriate and consistent with the duties of the employee. Section 14.2 of the AUP outlines expectations of City management.

Technology resource users*: Roles and Responsibilities*

All technology resource users are expected to understand and comply with existing laws and City bylaws, policies and standards, e.g.

Freedom of Information and Protection of Privacy (FOIP);

The City of Calgary's Administrative Policy Library including:

- Code of Conduct
- Respectful Workplace
- Conflict of Interest
- Public Statements and Media Relations
- Information Management

Along with any related or applicable Council policies, e.g. Calgary Corporate Accessibility Policy CSPS003

Administration policies are approved by the Administration Leadership Team (ALT), focus on the internal workings of The City as a corporation, and primarily impact and address City employees. They state the minimum standards employees and authorized technology resource users must follow.

Safeguarding assets and information

The City believes that when it comes to using and managing the acceptable use of The City's technology resources, we're all responsible. When using and managing City technology resources, technology resource users are expected to do so in a proficient, safe and acceptable manner:

1. Use of strong passwords and the frequent changing of passwords. Password standards
2. Safeguard technology devices from abuse or theft, and unauthorized access (e.g. store mobile devices in vehicles only if necessary and in a safe storage location that is out of the elements (cold, heat, rain, etc.) and out of view). Technology resources users are to:
    - Sign-out of their network account, remove the device and/or lock the device when leaving a computer, laptop or mobile device.
3. Safeguard assets and information (e.g. spreadsheets, programs, information, data, etc.) from abuse or theft. For example, all files and information are stored on a City network location, not a local drive.
4. Safeguard City assets and information by following The City's Cloud Solutions *Risk Value Assessment* evaluation.
    - Access to cloud solutions are to be secured to the same level as if this solution were hosted within The City's technology environment.
    - Cloud solutions must enable data captured by that vendor's solution to be transferred back to the City's data storage environment.

Responsible use of Removable Media

The increasing numbers of flexible workers has led to the need to have access to information regardless of the location of the worker or the device being used. The use of removable media for temporary storage of information has increased. Some examples of removable media include, but are not limited to: USB sticks (thumb drives), external hard drives, DVDs, memory cards and devices with their own storage capabilities such as laptops, tablets and smartphones.

1. City information with an Information Security Classification (ISC) of Unrestricted may be stored on removable media.
2. This information must be stored on a City network drive at the earliest opportunity where it is backed-up and protected and completely deleted from the removable media device.

Personal Use of City Network and Data Storage Services

1. Streaming of Council meetings, learning and world events is acceptable where your supervisor or manager agrees to the viewing of this event.
2. Check with your supervisor or manager if it is acceptable to store a personal file(s) on City technology computers or devices.

Personal Use of City Technology Resources

- The City understands and allows for a reasonable amount of personal use. If technology resource users have any questions about what this might mean or looks like, they are to discuss this with City management. Technology resource users, along with City management, are responsible for exercising good judgment regarding the reasonableness of personal use of technology resources, ensuring that the following principles are adhered to:
    - This personal use must not interfere with the overall performance of job duties.
    - Personal use should preferably take place during regular break times or before or after working hours.
    - There shall not be any expectation of privacy.
    - Any and all activity can be tracked and/or audited.
    - The City can and will block access to sites it deems inappropriate or dangerous. However, users should understand that just because a site has not been blocked it may still not be acceptable to access that site.
    - Personal use of City technology resources should not result in being a cost to The City.

For specific cases where access to a blocked site is required for business purposes, a user's immediate City manager will contact Corporate Security, who may provide this exceptional access on reasonable justification.

Examples of Acceptable Use:

1. Work-related web sites
2. Educational and other applicable web sites that further an employee's work knowledge and skills
3. Reading of online newspapers
4. Streaming of Council meetings or eLearning events
5. Limited Social Networking

Examples of Unacceptable Use:

1. Creating or accessing pornographic, obscene, indecent or sexually explicit material
2. Creating or accessing offensive material
3. Online gambling
4. Using the Internet for personal commercial purposes
5. Downloading commercial software or any copyrighted materials
6. Buying hardware, software and software services outside of normal City purchasing processes
7. Posting confidential, defamatory, harassing or knowingly false material
8. Using City storage for non City data
9. Emailing City documents or information to personal email accounts

Mobile Device Management

Mobile devices enable City technology resource users to work from anywhere. There are a few things employees can do to help protect and secure The City's mobile devices and the information on the devices. For more information refer to myCity (Mobile Device Management).

Actions mobile technology users shall follow:

1. Don't leave mobile devices unattended.
2. Report lost or stolen mobile devices to the IT Service Desk ITSHD at 403-268-8008.

Electronic Communication Services Use and Monitoring

City technology systems have been implemented to automatically monitor incoming electronic communication messages for unsafe/unwanted messages or attachments.

1. Any electronic communication messages deemed to be unsafe or unwanted will be blocked and removed to protect The City's technology systems.
2. Any investigation / monitoring requests must be made through Corporate Security.

City Technology Resource Use for Outside Activities

Technology resource users are encouraged to participate in community-based activities on their own time. Should there be a need to use The City's technology resources, this is allowed only with prior permission of the manager of his or her business unit and if the following policy conditions are met:

1. The activities are not to sell or promote a commercial third-party product or service
2. The activity is related to, but not limited to, involvement with charitable organizations, community service and professional organizations.

Disposal of City Technology Resources

All City technology devices or products are to be decommissioned or returned to The City for proper disposal. Asset management systems need to be maintained and updated.

For disposing of mobile devices, employees shall follow the process below. This ensures that the protection and integrity of the City's information is maintained and that all billing for the device is stopped. Detailed disposal requirements can be found on myCity (Device Disposal).

Use of Personal Devices

Due to significant risk of harm, loss of information and/or damage to the complex layers of technology, The City does not permit personal technology devices to be connected to its protected technology environment, except where enabled through remote secure access. This includes, but is not limited to:

1. Tablets, laptops
2. Smartphones, cell phones
3. Personal computers, peripheral devices such as USBs, DVDs/DVD players, external memory devices, etc.

City Support of Personal Devices

The City does not manage, support or reimburse for personally-owned technology resources (e.g. personal handheld wireless devices and airtime, ISP connections, home computers or home use software, etc.).

City Management's Responsibilities

City management is responsible for making sure that staff reporting to them are:

1. Informed and aware of the AUP policy and standards, and are adhering to them;
2. Provided with appropriate access to the technology resources they require to execute their role;
3. Demonstrate responsible usage of technology resources.

Further, City management is to:

1. Ensure that access and use of technology is provided as appropriate to the employee's role as a technology resource user;
2. Ensure access is terminated as soon as appropriate, when roles change or employment ends;
3. Review and approve City's technology resource purchases;
4. Monitor wireless usage and charges;
5. Provide City technology resource users with access to necessary training to proficiently use technology resources;
6. Approve technology resource users' access to City's technology resources while vacationing or away on City business, as necessary;
7. Update technology resource inventories and asset tracking in the event of human resource changes (i.e. new hire, transfer, resignation, termination or retirement).

Electronic Communications Services and Monitoring

City management should remind their technology resource users that if they receive any electronic communication message that is not in accordance with policy, to advise City management.

1. If City management requires technical assistance to stop continued receipt of this type of electronic communication message, he or she is to submit an IT Service Desk ticket or contact

Corporate Security for instructions on blocking the originator of the communication. *Please note: not all types of electronic communication messages can be blocked.*

Investigating and Reporting Policy Breaches

To determine if a violation of the AUP has occurred, management should consult with IT, HR and/or Law-Corporate Security. City management:

1. Initiates investigation of potential breaches of the AUP by following the Code of Conduct investigation escalation process (currently under development).
2. Consults with HR Business Advisory Services to ensure a consistent approach to investigations, to determine whether Corporate Security and/or IT need to be involved and to determine the appropriate response/action.
3. Informs the business unit Director of any breach of the AUP policy.
4. Takes appropriate action in response to any breach of the policy.

Investigation of policy breach

City management concerned about potential breaches of the AUP are to notify Human Resources Business Advisory Services (BAS) of their concern. Management will work with HR to determine whether to conduct an investigation or whether Corporate Security and/or IT will investigate the potential breach. If a breach is confirmed, management will work with HR to determine the appropriate response (e.g. non-disciplinary or disciplinary letter), in accordance with the Labour Relations Policy (HR-LR-002) or the Exempt Staff Policy (HR-LR-006).

General Principles for Use of The City's Technology Resources

Each position within The City has a defined role. Management assesses the tools and resources required for that role to effectively and efficiently perform the duties as assigned. The tools and resources include the technology resources required to perform that role or the intended purpose when executing that role on behalf of The City of Calgary.

Provisioning of technology resources for employees and contractors comes at a cost to the business within which the employee or contractor works or is assigned to work. These expenses must be justified and have an associated budget.

1. In most cases these budgets are allocated from tax dollars or service fees.
2. As such, it should not be assumed that every role will receive technology resources.
3. City management determines what technology resources provided are appropriate to the role.

Teleworking

Advancements in technology capabilities enable staff to work from a City of Calgary facility, telework from home or another location.

1. Employees are expected to adhere to the Acceptable Use of City Technology Resources Policy at all times, and from all locations.
2. Management must approve the working arrangement and be aware of the locations from which the technology resource user is working.
3. For more information, go to: Eligibility For Telework; Flexible Work Options

Internet Use and Monitoring

Corporate Security and IT employ a variety of tools to protect The City's electronic systems. City technology automatically records all internet sites visited by internal network users, identified by their computer account (technology resource user's online identity). This information is used to analyze patterns of each activity to alert Corporate Security of potential system risks and to assess compliance with the policy. Corporate Security will review patterns of policy non-compliance logged for a specific account.

To reduce the incidents of access to unacceptable internet sites and reduce the risk of phishing or hacking, Corporate Security will:

1. Determine which sites are to be blocked in accordance with the policy.
2. Use technology to block some web sites that are clearly not in keeping with the policy.

When an attempt is made to access a blocked site:

1. The City's technology resource user will be notified that access to this site contravenes the *Acceptable Use of City's Technology Resources Policy*.
2. Repeated attempts to access a blocked site will be logged.
3. A quarterly report of blocked internet access attempts is reviewed by Corporate Security.

Enforcement Considerations

The City's technology resources are valuable resources. It is important that The City identify who uses a specific technology resource and that the use is acceptable for City business purposes.

Shared/generic account usage:

As tracking of internet and email use is done based on a computer account tied to that activity, the "owner" of the shared account is responsible for any inappropriate activities initiated from that account.

1. To avoid confusion over the identity of The City's technology resource user in relation to shared computer accounts, City management shall encourage the use of individual (rather than shared) computer accounts, unless this will have an unacceptable impact on business efficiency.
2. To ensure only those that really require access to a shared or generic account, a yearly review of the need for that account will be undertaken.

Policy Governance Roles and Responsibilities

The AUP is an administrative policy approved by the Administrative Leadership Team (ALT). ALT policies provide a minimum standard applied to employee behaviours.

Information Technology (IT) is responsible for managing the Acceptable Use of City Technology Resources Policy (AUP). IT is supported by Law-Corporate Security, Human Resources (HR), and in some cases Customer Service & Communications (CSC) in meeting this responsibility.

The Information Management and Security Governance Committee provide senior management oversight to the implementation of the policy as outlined in these standards.

Information Management and Security Governance Committee (IMSGC)

The IMSGC is responsible for making decisions regarding information management, security and the acceptable use of technology resources at The City of Calgary in accordance with the IMSGC Terms of Reference. This committee:

1. Facilitates the implementation of policies they are responsible for across the corporation;
2. Provides technical, regulatory and policy leadership, including the approval and reviewing of related standards; and
3. Serves as a final escalation body when hearing appeals to decisions made by the various parties responsible for the administration of this policy and its standards.

Chief Information Technology Officer (CITO)

As the Director of IT, the CITO leads the Information Technology (IT) business unit as it provides the technology used to deliver all City services to Calgarians. This goes beyond providing staff with technology such as computers, software and mobile devices. As a corporate service, IT City works with departments in leveraging the use of technology for operational efficiencies and safeguarding The City network to protect corporate technology and information assets.

Relative to the AUP, the CITO:

- Chairs the IMSGC committee;
- Ensures that information technology investments align with the strategic goals of The City;
- Ensures that information security design is part of all system and infrastructure architecture design;
- Develops a process to identify opportunities for information sharing and embedding that process into IT development methodologies and business practices;
- Ensures that information technology plans are in place to enable business continuity; and
- Facilitates policy and standard revisions, ensuring these remain relevant and up-to-date reflecting current and future technology capabilities, uses and practices.

Law, Corporate Security, Chief Security Officer

Corporate Security, in relation to the AUP, is corporately responsible for information security and the security of technology business systems, devices, and infrastructure.

- Consults on requirements for new technology initiatives and projects;
- Provides technical resources for investigations;
- Advises on:
    - Information Security Classification and Acceptable Use of Technology issues;
    - Data storage for confidential and highly-restricted information;
    - Internet blocking and auditing systems;
- Performs regular vulnerability scans;
- Administers remote access authentication systems and anti-virus systems.

Human Resources (HR)

As outlined above, the AUP outlines the expected behaviours of employees' use of City technology resources. Leaders are encouraged to work with their Business Advisory Services (BAS) HR Business Partner to facilitate the investigation of a breach of acceptable use of City technology resources. BAS will consult with Labour Relations on an as-needed basis. HR will work with Law-Corporate Security and/or IT.

HR considers which, if any, document(s) is involved and must be followed. Not doing so may expose the corporation to significant risk including financial awards for damages, loss of reputation, strained relationships with unions, decreased employee engagement and more. Examples of documents include: collective agreements, City Policies, human rights or privacy legislation. Please reference the HR Governance website for more information on compliance.Examples of documents include: collective agreements; human rights or privacy legislation, etc.

HR is also responsible to ensure City management follows The City's investigation and discipline processes to ensure we are fair and consistent. For more information, speak to you HR BAS Business Partner, look at LR Policy (HR-LR-002), or take part in the *Leading in a Unionized Environment* LFME course.

Monitoring Policy and Standards

There is a Corporate requirement for reporting the nature and type of technology risks and AUP investigations and outcomes. Policy and Standard revisions are motivated when technology changes, and as a result of investigations.

- Reporting process is evolving and being matured as part of the overall Code of Conduct implementation program.
- Ongoing reporting is at a summary level, respecting individual privacy.
- Reporting will be done with input from IT, Law-Corporate Security and HR.

Interpretation and the AUP Policy and Standard

For clarification or interpretation of the AUP Policy, Standard, or of a potential technology risk, contact the IT Manager, Operations, or IT Manager, Innovation & Collaboration.

- IT will inform and/or consult with HR and Law-Corporate Security for clarity of understanding and/or interpretation.

Appendix 1 - AUP & AUP Standards Definitions

The City's Technology Resources are defined as being, but not limited to:

- Cloud computing– a style of computing where scalable IT-related capabilities are provided 'as a service' to using web-based technologies
- Electronic communications – examples of this would be, but not limited to, email, instant messaging, texting, social media, etc.
- Information - Any collection of data that is processed, analyzed, interpreted, classified or communicated in order to serve a useful purpose, present facts, or represent knowledge; an individual record or collection of records
- Mobile computing – devices which use wireless technology (e.g. cellular or Wi-Fi technology) to connect to The City's network including, but not limited to, notebook computers, laptops, tablets, cell phones, smart phones, air cards, radios and modems
- Network account - identifies an authorized user enabling them to access applications, shared drives, databases and systems connected to The City network
- Removable media – any physical media storage device that is used to temporarily connect to The City's network to copy and store information including, but not limited to, USB sticks (thumb drives), external hard drives, DVDs, memory cards and devices with their own storage capability such as tablets and smartphones
- Social Media – an internet-based communication tool with a focus on immediacy, interactivity, user participation and information sharing. Social Media includes social networking sites, forums, weblogs, wikis, online chat sites, video/photo sharing sites, etc.
- Technology Resources – include, but are not limited to, software, software services, and hardware such as: desk phones, printers, scanners, storage systems and devices
- Technology Resource User – include, but are not limited to: City of Calgary employees, vendors, contractors, consultants and any other individuals with authorized access to and use of The City's technology resources

Appendix 2 - Relevant Legislation and Bylaw

- FOIP Act of Alberta which includes coverage of:
    - Personal information must be protected in accordance with this law,
    - Implications for accessing private information for non-work related reasons,
    - Freedom of information requests can apply to any information in The City's custody, wherever it is stored, even on removable media or on personal devices, and
    - As a consequence of this Act, personal information may not be stored on removable media.
- Similarly to FOIP or other regulatory requests for information, legal discovery has the potential to access any information in The City's custody, regardless of where this is held. This includes any device, including removable media, on which City information has been stored. This could also mean an employee's home PC, laptop, phone or any personal device if City information has been stored there.
- The Records Management Bylaw (Bylaw 53M99) which requires compliance with Records Management policies and guidelines.

Appendix 3 - Relevant Administrative Policies

The following are the related administration policies:

- Acceptable Use of City Technology Resources (IM-IT-002)
- Code of Conduct Pamphlet
- Code of Conduct (HR-LR-005)
- Social Media, Media Relations and Public Statements (MP-001)
- Labour Relations Policy (HR-LR-002)
- Exempt Staff Policy (HR-LR-006)
- FOIP Employee Reference Manual
- Information Security Classification and Control (IM-IT-001).
- Records Management Program Mandate and Responsibilities (GN-011)
- Electronic Records Management (GN-015)
- Transitory Records Management (GN-016)
- Archival Records Management (GN-017)

Appendix 4 - Related Administrative Standards and Guidelines

- Information Principles Guideline
- Information Roles & Responsibilities Guideline
- Flexible Work Resources
    - About Teleworking
    - Technology for Teleworking
    - Managing your information