Policy

Title: INFORMATION TECHNOLOGY AND ACCEPTABLE USE POLICY			Number: 0163
Reference: Administrative Committee - April 11, 2018 Administrative Committee - June 6, 2018 Corporate Services Committee - June 12, 2018	**Adopted by City Council**: June 18, 2018 City Clerk	Chief Administrative Officer	**Supersedes**: Policy 0135 April 2009
Prepared by: Information & Computer Services, Corporate Services Division			

STATEMENT

THE CITY OF MEDICINE HAT (THE CITY) REQUIRES A SAFE AND EFFECTIVE COMPUTING ENVIRONMENT TO PROTECT THE CITY'S INFORMATION ASSETS AND ONLINE SERVICES. THIS POLICY INFORMS AND PROTECTS ALL STAKEHOLDERS AND USERS OF THE CITY'S NETWORK AND INFORMATION SYSTEMS BY COMMUNICATING ITS ACCEPTABLE USE OF CITY INFORMATION SYSTEMS.

PRINCIPLES

1. The City's information and IT resources are valuable assets that require responsible care and diligence to prevent abuse, theft, and Cybersecurity Incidents.
2. Limiting access to and use of City IT resources can mitigate the risk of Cybersecurity Incidents and prevent the use of City information and technology resources for inappropriate purposes.
3. Devices that connect to the City Network or are used for City business purposes, such as mobile phones, tablets, laptops, and other connected devices, removable media (such as USB drives), must comply with the acceptable use policy.
4. Cloud and Outsourced Vendor Technology solutions, are subject to approval by ICS prior to implementation and must comply with the acceptable use policy.

ROLE OF COUNCIL

1. To receive, review and adopt this policy and any recommended amendments thereto.

1. DEFINITIONS

1.01 Authorized Users - individuals who have been authorized to connect to City Network or City IT and includes remote access and/or third party users approved by the appropriate City authority.

1.02 CASL – An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c 23 (also known as Canada's Anti-Spam Legislation).

1.03 City Network – all the networks, technical infrastructure, applications and end user technology that is connected, owned and/or operated by the City.

1.04 Cloud – IT services offered where the location of the computing infrastructure is not located in the City's facilities.

1.05 Cybersecurity - a set of techniques used to protect the integrity of networks, programs and data from Cybersecurity Incidents.

1.06 Cybersecurity Incident – includes attempts (either failed or successful) to gain unauthorized access to a system or its data; unwanted disruption or denial of service; the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the City's knowledge, instruction, or consent.

1.07 Device – any item, including personally owned, City owned and publicly owned, capable of connecting to the City Network, including mobile phones, desktops, tablets, laptops USB keys and any removable media.

1.08 Electronic Communications – communications including messaging, voice, Internet browsing logs, audit logs, video, email and other documents created, sent or received using the City Network.

1.09 IT – Information Technology.

1.10 Network Data – any data created, received or sent using the City Network.

1.11 Outsourced Vendor Technology - any IT service not provided by a City employee.

1.12 Personal Information - recorded information about an identifiable individual as defined in FOIP Act.

1.13 Third-Party Service Provider – any third party offering a service that may affect the City Network.

1.14 Unauthorized Activities - sending or posting discriminatory, harassing, or threatening messages or images; perpetrating any form of fraud or theft; using, or disclosing someone else's password without authorization; downloading, copying or pirating software, film,

music or electronic files that are copyrighted without authorization; sharing confidential material, trade secrets, or proprietary information outside of the organization without authorization; accessing unauthorized websites; sending, posting or intentionally accessing information that is defamatory to the City, its products/services, colleagues or customers; introducing malicious software onto the City Network; jeopardizing the Cybersecurity of the City Network; sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities without authorization.

1.15 Unauthorized Content - material that intimidates, threatens, humiliates or discriminates against any individual or group; pornographic content; defamatory references or depictions.

2. RESPONSIBILITIES

2.01 City Council

(a) Receive, review and adopt this policy and any recommended amendments thereto.

2.02 Administrative Committee

(a) Review and adopt procedures which are developed for the implementation of this policy.

(b) Monitor the application, interpretation and administration of this policy.

2.03 Commissioners

(a) Ensure that managers and supervisors manage the authorized use of the City Network in their respective departments.

(b) Ensure that all employees and third parties in their division who are Authorized Users have had the opportunity to read this policy and obtain clarification on this policy.

2.04 General Managers/Management

(a) Determine which of their employees and third parties operating in their division are required to be Authorized Users.

(b) Determine which City Network capabilities and Devices each of their employees and third parties operating in their division will be authorized to access.

(c) Ensure that all employees and third parties operating in their division who are Authorized Users have had the opportunity to read this policy and obtain clarification on this policy.

(d) When a complaint/concern is received, take appropriate steps to investigate. This may include consulting with GM, ICS and GM, Human Resources.

(e) If an employee or third party operating in their division violates this policy, pursue the appropriate disciplinary action.

2.05 General Manager ICS/General Manager Human Resources

(f) Consider requests for access modifications or acceptable use reviews.

(g) Considers potential breach investigations on Authorized Users as requested from a General Manager.

(h) When a complaint/concern is being investigated, provide assistance with investigative process, as required, to ensure that a fair and confidential investigation is conducted.

2.06 Information and Computer Services (ICS)

(a) Provide information security awareness training tools and solutions.

(b) Employ technology systems, activity logs, performance analyzers, data recovery and archival tools, monitoring and filtering tools, and visual confirmation as a means of tracking and documenting violations of this policy.

(c) Assess and approve software or hardware for use on, or connecting with, the City Network.

(d) Provide City Network usage/audit information as requested and required to Human Resources.

2.07 City Employees/Authorized Users

(a) Use the City Network in a responsible, ethical, law-abiding manner.

(b) Acknowledge that the City may monitor the City Network, and Devices connecting to the City Network.

(c) Understand that Electronic Communications pursuant to employment and/or a contract with the City are considered the City's property.

(d) Make use of the City's resources and training in Cybersecurity and make informed, security-conscious decisions.

(e) Report suspected Cybersecurity breaches or potential Cybersecurity Incidents to their immediate supervisor and ICS Service Desk.

(f) Protect City information, such as account credentials, passwords, electronic information, and other information assets in regards to the City Network.

(g) Consult with ICS for Cybersecurity guidance when using Cloud services, or Third-party Service Providers.

(h) Understand that employees may engage in limited personal use of City information technology, in accordance with the Code of Ethics, but that all City Network data may be monitored and personal use must not impact the functioning of the City Network.

(i) Understand that all information and intellectual property created by or on the City Network, are records for the purposes of the Freedom of Information and Protection of Privacy Act and may be accessible to the public pursuant to the provisions of that Act.

3. PROCEDURES

3.01 An Authorized User may use only the City owned Devices, user accounts, and electronic files for which authorization has been granted. Authorized Users are individually responsible for appropriate use of all assigned City resources, including City owned Devices, network addresses, electronic files, software and hardware.

3.02 Authorized Users should make every reasonable effort to protect passwords and to secure resources against unauthorized use or access.

3.03 Authorized Users are expected to review training and further information available on the City Information and Computer Services intranet site.

3.04 Authorized Users are expected to be professional and respectful when using City owned Devices and user accounts to communicate with others; the use of City Network to libel, slander, or harass any other person is not allowed and could lead to disciplinary action.

3.05 When sending mass emails (more than 1 recipient) external to the City Network, Authorized Users are expected to use the "Bcc" function whenever reasonably possible, instead of the "To" or "Cc" function to protect recipients' privacy.

3.06 Although City does not actively monitor or limit content of information transmitted on the City Network, it reserves the right to access and review such information under certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy (with reasonable cause), or to ensure that the City is not subject to claims of misconduct.

3.07 While every effort is made to insure the privacy of City email users, this may not always be possible. In addition, since Authorized Users are granted use of the City Network to conduct City business, there may be instances when the City, based on approval from the employee supervisor at a Manager level or higher and the General Manager of Human Resources, reserves and retains the right to access and inspect any stored information without the consent of the user.

3.08 Access to an Authorized User files/emails may be granted to someone other than the Authorized User only when there is a valid reason to access those files. Authority to access files/email can only come from the Authorized User's manager and must be approved by the General Manager of Human Resources.

3.09 Any individual who willfully or purposefully does not abide by the sections that pertain to them is considered to be in violation of this policy. Using the City Network for the following purposes is considered a violation of this policy:

(a) Intentionally accessing any Unauthorized Content or performing any Unauthorized Activities.

(b) Violating copyright or intellectual property laws.

(c) Breaching the City's Code of Ethics.

(d) Conducting business activities unrelated to City employment or contract for personal gain.

(e) Unauthorized access, use or disclosure of personal information, confidential information, or proprietary data belonging to the City or another person or entity with whom the City conducts business.

(f) Accessing or attempting to access another user's account or Cloud service without authorization.

(g) Installing unlicensed or unauthorized content.

(h) Breaching any international, federal, provincial or local law, including the Freedom of Information and Protection of Privacy Act (Alberta) and CASL.

(i) Connecting any Device that is not owned by the City to the City Network without authorization.

3.10 All requests, questions, concerns, breaches or suspected breaches should be reported to your direct supervisor and the ICS Service Desk.

3.11 Any violations of this policy may be subject to disciplinary action.