Policy

Title: CYBERSECURITY POLICY			**Number**: 0164
Reference: Administrative Committee - April 11, 2018 Administrative Committee - June 6, 2018 Corporate Services Committee - June 12, 2018	**Adopted by City Council**: June 18, 2018		**Supersedes**:
	City Clerk	Chief Administrative Officer	
Prepared by: Information & Computer Services, Corporate Services Division			

STATEMENT

INFORMATION, AND INFORMATION SYSTEMS ARE CRITICAL ASSETS TO THE CITY OF MEDICINE HAT. THE CITY HAS A CYBERSECURITY PROGRAM (INFORMATION SECURITY PROGRAM) TO ENSURE INFORMATION IS PROTECTED IN ACCORDANCE WITH ITS CRITICALITY, SENSITIVITY, AND RISKS.

PRINCIPLES

1. In the City's high value IT landscape, sophisticated and significant Cybersecurity risks are present. The City has a need for a Cybersecurity Program.

2. IT services, vendors and infrastructure are primary targets and must be protected in accordance with the Cybersecurity Program described in this policy.

3. The City's Cybersecurity Program will be based on the National Institute of Standards and Technology ("NIST") Cyber Security Framework.

4. This policy describes the Citywide collective responsibility towards Cybersecurity. Many of the threats to the City's Cybersecurity are sophisticated and targeted at varied organizational levels across departments necessitating broad organizational commitment and participation.

5. Not all City departments or City corporations have the same technological implementations. Many operate independent technologies and work in regulated environments. This policy does not supersede obligations, regulations, or regulated reporting requirements, but will introduce integrated processes and practices such as incident reporting and compliance validation.

ROLE OF COUNCIL

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

1. DEFINITIONS

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

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

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

1.04 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.

1.05 Cybersecurity Manual – describes the standards and processes for Cybersecurity on shared IT systems, networks and Cloud, and provides a Citywide reference baseline standard.

1.06 Cybersecurity Program – a program focused on the protection of IT systems, including City Network security and the City's ability to prevent, detect, and respond to Cybersecurity Incidents. The Cybersecurity Program is based on the NIST Cybersecurity Framework.

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 ICS Risk Register – a prioritized listing of all major risks with respect to IT and Cybersecurity.

1.09 IT – Information Technology

1.10 Incident Response Plan - set of written processes and instructions for coordinated implementation of incident detection, response and recovery for Cybersecurity Incidents. It is part of an overall Cybersecurity Program.

1.11 NIST (National Institute of Standards and Technology) Cybersecurity Framework - an established reference model and standard to establish, measure, and define a Cybersecurity Program. It includes:

(a) Risk Identification which considers the criticality and sensitivity of City information, systems, Cybersecurity threats and vulnerabilities.

(b) Information Protection which considers technical safeguards (such as encryption), vulnerability management (such as patching and hardening), Operational practices in IT operations and application development, and repeatable processes; information governance.

(c) Recovery results in continuous risk management, continuous improvement of protection and maturity improvements.

1.12 Payment Card Industry (PCI) - the segment of the financial industry that governs the use of all electronic forms of payment.

1.13 Supervisory Control And Data Acquisition (SCADA) - is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management.

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 including the Cyber Security Manual.

2.03 Chief Administrative Officer

(a) Ensure compliance with the Administrative Organization Bylaw in the implementation of this Policy.

(b) Without limiting the general statement in (a), delegate the powers, duties and functions of the Chief Administrative Officer pursuant to the Administrative Organization Bylaw to City employees as necessary to give effect to this Policy.

2.04 Commissioner of Corporate Services

(a) Establish and maintain the Cybersecurity Program to ensure City electronic information and the City Network are adequately protected.

(b) Report annually to City Council regarding key risks, compliance, and significant activities in relation to the City's Cybersecurity Program.

2.05 General Managers/Management

(a) Oversee departmental access to, and use of, the City Network, information, IT and information systems, including access and use by vendors, consultants, and volunteers.

(b) Support implementation of, and compliance with, the Cybersecurity Program and policies related to Cybersecurity.

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

(d) Ensure all third party applications (including Cloud based or hosted services) are approved by the GM, ICS.

(e) Submit annual compliance report and risk mitigation strategies to the General Manager of ICS with respect to the Cybersecurity of the technology operated by their business units not under the direct control of ICS, such as SCADA and PCI.

(f) Work with ICS as a Cybersecurity partner in the implementation of Citywide Cybersecurity Incident response in accordance with the City's Cybersecurity Incident Response Plan.

(g) Report all suspected and real Cybersecurity vulnerabilities and incidents to the ICS Service Desk.

2.06 General Manager, Information and Computer Services

(a) Implement, operate and manage the Cybersecurity Program, including policies, tools, and reporting related to Cybersecurity, and the Cyber Security Manual.

(b) Prepare an annual report on key risk indicators, business unit compliance and activities in relation to Cybersecurity.

(c) Conduct an annual Cybersecurity assessment against the NIST standards.

(d) Manage Citywide Cybersecurity Incident response in coordination with department heads.

(e) Manage Cybersecurity operations of the City Network, shared IT systems and connections, Cloud and third party information providers.

(f) Work as the Cybersecurity partner for all City departments and entities, and develop and maintain the Cybersecurity Manual, and Cybersecurity operations.

2.07 Information and Computer Services Employees

(a) Identify, detect and respond to Cybersecurity Incidents and implement recovery and protective measures in relation to Cybersecurity Incidents, as assigned by ICS Management.

(b) Operate the Cybersecurity Program with dedicated responsibilities in Cybersecurity Incident handling, and Cybersecurity operations, as assigned by ICS Management.

(c) Maintain the Citywide ICS Risk register and IT risk management process, as assigned by ICS Management.

(d) Maintain the Cybersecurity Manual, and support standards and processes, as assigned by ICS Management.

2.08 All Employees

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

(b) Comply with the applicable provisions of the Cybersecurity Manual.

3. PROCEDURES

3.01 Exceptions to this policy must be approved by the Commissioner, Corporate Services and the appropriate General Manager. A request for an exception to this policy can be made by a department or vendor and in each case, the request must be in writing and include all material information regarding the request, including the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and General Manager approval for the exception.

Cybersecurity Program procedures and standards will be defined in the Cybersecurity Manual. Contents of the Cybersecurity Manual include:

A. Risk Identification
  - a. Asset Classification
  - b. Risk Assessment
  - c. Cloud and Third Party
  - d. Dashboard and Reporting

B. Information Protection
  - a. Access Control
  - b. Identification & Authorization
  - c. Patch Management
  - d. Vulnerability Management
  - e. Perimeter Security
  - f. Data Retention
  - g. Network Protection
  - h. Malicious Code Prevention
  - i. Encryption

C. Incident Detection, Response and Recovery
  - a. Incident Detection
  - b. Incident Response Playbooks
  - c. Security Logging
  - d. Incident Recovery

D. Application Security

E. Data Centre Security

F. Compliance
  - a. PCI
  - b. Regulatory
  - c. Privacy and Information Protection

G. Index of Standard Operating Procedures