TheCounty

PRINCE EDWARD COUNTY ◆ ONTARIO

Title: Information Technology Security Policy	
Policy Group: **Your Government and People**	**Policy Administrator:** **Information Technology**
Resolution No. **CW-119-2022**	**Policy Number:** **IT-01**
Approval Date: **2022-05-12**	**Revision Date:** **2023-05-12**

1. Policy Statement

a. This Information Technology Security Policy is designed to ensure that the County operates a secure and reliable technology environment, with adequate controls to protect the County’s information assets.

2. Purpose

a. The objectives of this Policy are to:
- Clarify the provision and management of access controls to County network resources;
- Establish County password standards;
- Establish the County’s approach to securing the technology environment, through border controls, virus management and other best practices;
- Establish a security awareness training program;
- Establish appropriate physical controls for County IT resources;
- Clarify the County’s position on data security; and
- Establish procedures for performing investigations.

3. Scope

a. This policy applies to members of the County including members of Council, staff (full-time, part-time and contract), volunteers, Boards, external suppliers, contractors, consultants and anyone else utilizing or accessing the County's assets.

4. Legislative Authority

a. Not applicable.

5. Definitions

a. **Encryption** is a means of securing digital data using one or more mathematical techniques, along with a password or "key" used to decrypt the information. The encryption process translates information using an algorithm that makes the original information unreadable.

b. **IT infrastructure** means IT assets including, but not limited to, servers, databases, data, software, end-point devices, network, Internet connections, central authentication, the telephone system, and data centres, whether provided directly by IT or contracted.

c. **Server** means a computer or software/program that provides access/services to other computers/programs.

d. **Virus means** a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

e. **Controls** means procedures, processes, practices, or standards put in place to minimize risk.

f. **Secure facilities** means County data centres or secure hosted facilities, managed by the IT department.

6. General

a. All users must access and use IT services and IT infrastructure in ways that reduce and mitigate IT security risks.

b. The primary means of reducing and mitigating IT security risks for the County is by:
   i. All IT services, where practicable, to be administered by IT staff and hosted in secure facilities
   ii. All IT end-point devices, where practicable, must use services offered by IT to ensure compliance with IT security procedures.

c. To the extent that the primary means of reducing and mitigating IT security risks is not practicable, the secondary means is for the unit or individual to work with a security provider to implement alternative mitigation strategies to ensure that the overall risk to the County is being maintained at an acceptable level. The process by which this will be accomplished is identified in the IT Risk Management procedure.

d. The administration and management of
    i. IT Security Incident Response shall be in accordance with Appendix A;
    ii. IT Cloud and Hosted Solutions shall be in accordance with Appendix B;
    iii. Third party access shall be in accordance with Appendix C; and
    iv. Backup, disaster recovery and business continuity shall be in accordance with Appendix D.

7. Responsibility and Implementation

a. Council is responsible for approving this Policy.

b. The Chief Administrative Officer (CAO) in conjunction with the Manager of Information Technology is responsible for:
    i. directing compliance and resolving any conflicts with this Policy;
    ii. approving procedures; and
    iii. making routine or administrative changes to the Policy, as required.

c. All Directors, Managers, and Supervisors are responsible for:

    i. Ensuring all staff have read and understand the training materials provided to them, including any updates.
    ii. Ensuring that staff are compliant with this policy.
    iii. Ensuring that any violations of this policy are addressed and that proper coaching and/or disciplinary actions are taken.

d. All authorized users and the County's partners with regards to IT security, must:
    i. Helpdesk to provide internal support
    ii. Manager responsible for IT is responsible for providing training and the implementation of the Policy.

8. Documentation and Forms

a. The following are procedures related to this policy:
    - IT-01-01 IT Security Incident Response Procedures
    - IT-01-02 Information Technology Security Procedures
    - IT-01-03 Cloud and Hosted Solutions Procedures
    - IT-01-04 Backups Disaster and Business Continuity Procedures
    - IT-01-05 Data Centre / Secured Computer Room Access

Appendix A: IT Security Incident Response

1. The Security Incident Response protocol ensures that an orderly sequence is followed when an incident is declared. Additionally, it ensures that the right resources are involved in identifying and declaring a Security Incident.

2. The purpose of the following sections is to define IT department's roles and responsibilities for the investigation and response of computer security incidents and Data Breaches.

3. The process described in this document applies to the following:
    a. All Prince Edward County departments
    b. All business partners, and contractors handling or storing Prince Edward County Intellectual Property
    c. All such partners must agree to disclosure of any event relating to intellectual property or the facilities and systems processing or containing intellectual property (including peripheral systems such as infrastructure services) as per this process.

4. Incidents of an operational nature, involving infrastructure, or in any way not directly affecting the security of Intellectual Property or other sensitive information are not in scope and should be referred to the IT helpdesk.

5. This Policy does not apply to disasters such as fire or flood which are handled through the business continuity (BCP) and the disaster recovery (DR) plans.

6. Definitions

    a. Information Security Incident means any incident where there is knowledge or suspicion that the confidentiality, availability or integrity of Prince Edward County Information Assets has been compromised.

        i. In this document a Security or Information Security Incident refers to a directed attack intended to compromise the confidentiality, integrity, or availability of data as defined above. This is commonly referred to as a data breach or security breach. These events should not be confused with operational security events or incidents that take place commonly and are addressed by other processes and internal operational teams.

        ii. Some incidents such as Spam, Virus & Malware are known as operational security incidents and are handled via regular operational incident management (Helpdesk). A virus outbreak for example can have a major impact on the enterprise but is still considered an operational event unless the investigation performed by IT determines that the malicious code (virus) was collecting sensitive information therefor resulting in a Data Breach event.

Example 1: A user's workstation appears to be infected by a virus. In this example, the helpdesk can process this event as an operation event. During the course of the resolution of this event, if it is found that the virus in question allowed the control of the workstation remotely, or captured sensitive information, then this would become an incident to be managed using this incident management process.

Example 2: An IT team member observes unidentified network activity between the corporate network and Internet addresses in a foreign country not serviced by the enterprise. This should be processed through this incident management process.

iii. When in doubt, use this process.

iv. One of the Information Technology department's primary duties is to protect Prince Edward County's Intellectual Property. This process defines only incidents that are the responsibility of the IT Security team and therefore the definition of an Information Security Incident is an important one.

v. There are many types of security incidents, and this process does not apply to all of them.

b. Security incident means an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed. Examples include:

- unauthorized disclosure of sensitive information
- theft or loss of equipment that contain private or sensitive information
- extensive virus or malware outbreak and/or traffic
- repeated, purposeful attempts to gain unauthorized access to a system or it's data
- a compromised user account causing significant harm (e.g. ransomware)
- extensive disruption of the organization's information services

c. Intellectual Property means ANY Prince Edward County information or asset.

7. Data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.

8. The IT Security Team detects and investigates security events to determine whether an incident has occurred, and the extent, cause and damage of incidents.

9. The IT Manager & Security Team directs the recovery, containment and remediation of security incidents and may authorize and expedite changes to information systems necessary to do so. The IT Manager & Security Team coordinates response with external parties when existing agreements place responsibility for incident investigations on the external party.

10. During the conduct of security incident investigations, the IT Security Team is authorized to monitor relevant IT resources and retrieve communications and other relevant records of specific users of IT resources, including login session data and the content of individual communications without notice or further approval and in compliance with other relevant County Policies.

11. Any external disclosure of information regarding information security incidents must be reviewed and approved by the IT Manger in consultation with the CAO, Legal, Communications, and other departments as appropriate.

12. The IT Manager may coordinate with law enforcement, government agencies, and peer IT Security Teams in the identification and investigation of security incidents. The IT Manager is authorized to share external threat and incident information with these organizations.

13. The following are the roles and responsibilities of the employees of the Prince Edward County and its partners with regards to security incidents:

    i. All employees (Prince Edward County, contractors and partners) must declare any security event to the 1st line support (HelpDesk). Alternatively, after hours contact IT on call representative.

    ii. Helpdesk (Prince Edward County or contractors/partners 1st line internal support) shall:
        1. Receive, complete and record incident declarations.
        2. Perform a quick preliminary analysis to determine whether incident is security related. Escalate until determination can be made. Forward all Security Incidents to the IT Security team

    iii. Manager responsible for IT shall:

1. Promptly authorize expenditures for incident containment, response and investigation services.

iv. IT Department shall:

- Confirm, accept, and document Information Security incidents.
- Coordinate incident response, including containment.
- Collect or manage the collection of any evidence.
- Report Incident to management based on the documented severity and escalation flow chart
- Declare the incident closed (contained)
- Provide guidance in remediation and operational improvements.
- Follow up on agreed upon remediation and operational improvements
- Declare the event closed once agreed upon remediation and improvements are in place

v. Business Partners shall:

1. Properly declare relevant incidents per this process and its definitions.
2. Provide a point of contact for incident reporting and response.
3. Provide expertise and support as needed for incident handling and response.

vi. HR, External Legal, Procurement, Communications, Corporate Services shall:

1. Provide expertise and support in dealing with human resources, potential legal liabilities, contractual issues, and issues relating to the organization’s public image.

14. The procedures for the protocol are as follows:

- Process
- Process Design
- Process Workflow
- Post-Incident Handling Process Flow
- Security Level and Escalation
- Process Description

Appendix B: IT Cloud and Hosted Solutions

1. The IT Cloud and Hosted Solutions protocol outline best practices and approval processes for using Cloud computing services and Hosted Solutions at the County. The Policy is designed to enable the County to take full advantage of emerging Cloud computing capabilities in a way that ensures that the County's data and information can be appropriately managed and secured.

2. The purpose of this protocol is to:
    a. Clarify the County's position on Cloud computing;
    b. Establish the processes by which Cloud computing services should be procured;
    c. Establish the processes that the County will use to determine suitability and applicability of Cloud computing services; and
    d. Establish the position on using personal Cloud computing services.

3. Definitions

    a. Cloud computing means technology that allows users to access and use shared data and computing services via the Internet or a Virtual Private Network. It enables convenient, on-demand access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be provisioned and released without the County having to build infrastructure to support these resources within their own environment or network. There are three types of Cloud computing service models. This Policy covers all three of these Cloud computing service models. Note that the definition of Cloud is evolving rapidly and this definition should be reviewed annually:

        i. Software as a Service (SaaS) - The capability provided is for the County to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser. The County does not manage or control the underlying cloud infrastructure that runs the software including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

        ii. Infrastructure as a Service (IaaS) - The capability provided to the County is to provision processing (servers), storage, networks, and other fundamental computing resources where the County is able to deploy and run software, which can include operating systems and applications. The County does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

iii. Platform as a Service (PaaS) -The capability provided to the County is to deploy onto the cloud infrastructure County-created or acquired applications created using programming languages and tools supported by the provider. The County does not manage or control the underlying cloud infrastructure but has control over the deployed applications and possibly application hosting environment configurations.

3. The range of Cloud computing options available is rapidly increasing. The County has already implemented or is in the process of implementing a range of Cloud computing and should expect to implement an increasing number of Cloud computing services in future.

4. The County will continue to be open to using Cloud computing technology (including SaaS, PaaS, IaaS) when and where it is deemed appropriate, cost effective and where the technology can meet the County's required standards.

5. The Manager of IT is responsible for:

   i. the administration and management of practices in compliance with the principles set out in this Policy; and,
   ii. Reviewing this Policy, along with its associated procedures and guidelines, every four years, or earlier if needed, in order to ensure continuing relevance and conformance with best practices.

6. The following are procedures related to this policy:

   vii. Procuring Cloud Computing Services Procedures
   viii. Interim Data Classification Scheme Procedures
   ix. Privacy Impact Assessment Procedures
   x. Cloud Service Provider Requirements Procedures
   xi. Personal or Self- Provisioned Accounts Procedures

Appendix C: Third Party Access

1. The Third-Party Access Policy outlines responsibilities and expectations of any individual from an external source (contracted or otherwise) who requires access to the County network, information systems and/or IT facilities for the purpose of performing work.

2. The objectives of this policy are to:
   a) Provide clarification of expectations for third party's accessing county IT infrastructure
   b) Provide clarification of expectations for IT departments role
   c) Provide direction for departments engaging third parties to carry out work on County technology systems

3. This policy applies to all Employees, Contractors, and Third-Party Employees, who use, process, and manage information and business processes of Prince Edward County.

4. Third-party access refers to the process of an organization granting external vendors and service providers secure access to corporate IT assets for maintenance, administration and management purposes. The County relies on third-party vendors and managed service providers to support their internal IT systems, applications and infrastructure. Outside vendors and service organizations often require privileged access to on-premises and cloud-based IT systems and business applications to perform routine support and administrative functions.

5. The Senior IT Manager is responsible for providing training and the implementation of the policy. The Senior IT Manager is also responsible for the maintenance of the policy recommending changes if necessary.

6. The following are procedures related to this policy:
   a. Data Centre/Secured Computer Room Access

Appendix D: Backups, Disaster Recovery and Business Continuity

1. A backup is a copy of a program or file that is stored separately from the original. These duplicated copies of data on different storage media or additional hardware resources are used to restore the original after a data loss event. Backups are used primarily for two purposes. The most common is to restore small numbers of files after they have been accidently deleted or corrupted. The second is to restore a state following a disaster.

2. This policy defines the backup for computer systems that store County data. These systems are typically servers but are not necessarily limited to servers.

3. This policy is also designed to prevent the loss of County data in the event of an equipment failure or destruction.

4. The objectives of this policy and associated procedures are to:
   i. Establish the County's approach to backup and restore for corporate systems

   ii. Clarify the County's approach to backup and restore for desktop and other data stores

   iii. Clarify the County's position with regard to providing business continuity and disaster recovery services

   iv. All information stored electronically in computerized form must be backed up on a routine basis to ensure its safety in the event of a severe hardware interruption, software interruption, virus attack, or other disaster.

5. This policy applies to all IT systems or applications managed by the County of Prince Edward that store, process or transmit information, including network and computer hardware, software and applications

6. This policy does not apply to information that is stored locally by users on desktops, laptops, tablets and mobile phones. Device owners are responsible for appropriate backup of the data stored locally on their mobile devices, with the exception of data synchronized with the device and stored on County servers (such as Outlook emails and contacts).

7. Definitions

   a. Data Backup is a periodic copy of data for the purpose of being able to restore data in case of data loss

b. A DRP “Disaster Recovery Plan” is a documented set of procedures describing the key activities that are necessary to recover minimum IT services, applications and data to continue critical business operations, and to fully recover such operations after a disaster affecting normal IT services.

c. A business impact analysis (BIA) is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption.

8. The responsibilities are as follows:
    a. Council approve and formally support this policy
    b. CAO review and formally support this policy
    c. The Senior IT Manager is responsible for providing training and the implementation of the policy. The Senior IT Manager is also responsible for the maintenance of the policy recommending changes if necessary.

9. Procedures are as follows:
    a. Corporate Systems Backup
    b. Desktop, Laptop and non- Corporate Server Backup
    c. Retention
    d. Disaster Recovery & Business Impact Assessment