Corporate Policy

Policy: **Remote & Mobile Computing Policy**

Main Contact: **Clerk**

Last Revision: **New**

Policy Statement

Purpose

Definitions

Policy Requirements

Monitoring

Authority

Contact

Change History

Policy Statement

The Corporation of the Township of Whitewater Region permits remote and mobile computing.

Purpose

The Corporation of the Township of Whitewater Region shall ensure compliance with mobility and theft protection standards.

Definitions

In this policy, the following terms have the meanings set out below:

“Mobile Phones” mean any portable phone device that, in addition to having the capability to make and receive phone calls, is also capable of receiving, transmitting and/or storing confidential information.

“Confidential Information” means any individual’s Personally Identifiable Information (PII) and other information that is confidential in nature.

“External Storage Device” means any device that connects to an external interface of a computer, or to which data can be transferred. This includes, but is not limited to USB, eSata, Firewire, Bluetooth, and wireless devices.

“Remote Access” means any network access that uses any network that is not owned and controlled by the Township as part of the connection. This includes home networks and public networks, as defined below.

“Public Networks” means any network that is located in a public place and allows patrons, customers or other non-authenticated users to connect to the network.

“Township” means the Corporation of the Township of Whitewater Region.

Policy Requirements

1.0 General Provisions

1.1 All Township computer equipment security requirements are in effect for mobile phones. These requirements include, but are not limited to:

- Strong authentication
- Prohibition of installing unauthorized software
- Prohibition of modifying configuration settings.

1.2 The portable nature of mobile devices requires procedures which may not be applicable for workstations or similar computer equipment. These requirements include, but are not limited to:

- Report a lost or stolen mobile phone immediately;
- Keep your device in a secure location when not in use and never leave it unattended;
- Lock the device with a password or Personal Identification Number (PIN);
- Install Apps only from trusted sources;
- Back up your data;
- Keep your system updated;
- Do not hack (jail-break, root) your device;
- Log out of banking and shopping sites;
- Turn off Wi-Fi and Bluetooth services when not in use;
- Avoid sending personal information via Text or Email;
- Be careful what you click;
- Do not send confidential data over insecure (HTTP) connections;
- Do not connect to company resources from public networks (coffee shops, restaurants, libraries, airports, etc.).

2.0 Mobile Data, Stored Data

Appropriate measures to protect data stored on remote or mobile devices must be implemented.

3.0 Locations

Township Users shall use approved connection methods only when connecting from remote locations, including home networks, hotels, and public networks.

4.0 Remote Access Restrictions

The Township reserves the right to restrict, prevent, or otherwise control remote access to its network if the Township believes that such remote access is not being used in accordance with any directives, or is otherwise detrimental to the interests of the Township.

5.0 Approved Hardware and Software

Hardware and software configurations for remote access computers must meet the same requirements as set out for equipment used on Township premises. In particular, hardware and/or software that do not meet Township business requirements must not be installed. Any workstation, either laptop or desktop, with non-approved hardware/ software configurations must not connect to the Township's networks.

6.0 Access to Remote Information Processing Facilities

Access to any remote information processing facilities must be through VPN and in conformance with Township requirements.

6.1 VPN Cryptography

Remote access VPN must employ cryptography which is in conformance with good computing practices.

Monitoring

Any suspected security breach relating to remote access must be immediately reported to the Clerk and CAO.

Authority

Section 224 of the *Municipal Act, 2001* states the role of Council includes the development and evaluation of policies and programs of the municipality.

Contact

Clerk
P.O. Box 40, 44 Main Street
Cobden ON K0J 1K0
(613) 646-2282

Change History

Policy Name	Effective Date	Significant Changes	By-law No.
Remote & Mobile Computing Policy	October 1, 2019	New Policy	19-10-1215