Township of Brock Corporate Policy

Policy Name: Information Technology Employee Policy

Policy Type: Administrative

Policy Number:

Reference:

Date Approved:

Date Revised:

Approval By: (most cases Council)

Point of Contact: Manager IT

Policy Statement

The Corporation of the Township of Brock ('the Corporation') is committed to providing the required Information Technology devices and access in order to ensure staff have the necessary items to conduct business on behalf of the Corporation.

Purpose of the Policy

This policy provides guidelines for the protection and use of Corporation owned information technology assets and resources to ensure the integrity, confidentiality and availability of data and assets. In addition, this policy provides guidelines for the use of personally owned mobile devices accessing Corporation information.

Definitions

Device: means a desktop or laptop computer provided by the Corporation

Mobile Device: means a tablet, cellphone or other easily portable device

Software: means any installed program including applications on mobile devices

VOIP Phone: means Voice over Internet Protocol phone system including desktop phones and associated hardware including headsets

Network System: means cabling, hard wired connections, Wi-Fi connections, firewalls and/or associated switches and equipment

MFA: Means Multi-Factor Authentication

Policy

i. Corporation hardware devices and software remain the property of the Corporation.
ii. Corporation hardware devices, software programs and network systems purchased and provided by the Corporation, are to be used only for creating, researching, and processing Corporation related materials. Corporate laptops, desktops, VOIP phones, and other hardware are to be used solely for business purposes and activity on these devices may be logged. Performance of illegal activities such as downloading pirated materials through the Corporation network by any user, authorized or otherwise, is prohibited.
iii. All Corporation devices, including desktop and/or mobile devices, shall be kept in working condition as originally provided. Normal wear and tear do not apply to this section. Staff may be responsible for any hardware and/or software damage that occurs as a result of misuse or alterations.
iv. All Corporation computers and/or mobile devices are provided with a standard suite of software applications including, but not limited to:
    a. Microsoft Windows 10
    b. Microsoft Office 365 (Outlook, Excel, Word, Powerpoint)
    c. Microsoft Teams
    d. Adobe Reader
    e. Microsoft Internet Explorer or Microsoft Edge
    f. McAfee protection suite
v. Other specific software may also be installed including, but not limited to:
    a. Microsoft Dynamics (Great Plains)
    b. Ingenious Software (FirePro)
    c. CityView
    d. Crisys
vi. Employees requiring any hardware additions such as web-cameras, cd/dvd disk drives, scanners or printers should request through the department head. Purchasing of this equipment shall be approved through the Manager of IT unless the request is for a replacement of an existing hardware component of similar capabilities.
vii. Employees requiring any software additions or upgrades shall receive approval from the department head prior to downloading. Installation of most software requires administrator rights which are only given to Durham Region IT staff. IT Help request will be required to track the request and installation.
viii. Staff are responsible for ensuring all system and hardware updates as identified to be installed on any Corporate device are completed in a timely manner.
ix. No copies or duplication of any data including license keys, installation codes or similar items is permitted.
x. All data placed onto a memory stick or any other portable media device is encrypted using the Corporation supplied software and is treated with the same sensitivity and security as all other data and Corporate information. Sharing of this data is only permitted for Corporation business when not readily available to the other party through secured access to Corporation databases.
xi. Staff must ensure physical security of any Corporation device or mobile device and should ensure the device is locked when not in use and/or kept in a secure location.

xii. Maintaining the physical and electronic security of all data accessed or accessible on Corporation devices is the responsibility of all staff. Unauthorized access to data in any format is strictly prohibited.

xiii. All data including but not limited to emails, spreadsheets, scanned documents, software specific data and photos remain the property of the Corporation and are not to be purged or bulk deleted at any time without the express knowledge of the Department Head and/or Manager IT.

xiv. Security of the VOIP phone system including device based soft phones or mobile device applications as well as remote access to the VOIP phone system portal using provided username and/or password are the responsibility of all staff.

xv. The Corporation has installed security software including antivirus and web protection software. If you suspect a virus or any unauthorized access to your computer, contact the IT Help desk immediately.

xvi. If staff leave the employ of the Corporation for any reason, they shall return the original and/or any copies of all Corporation software, computer materials, device or mobile device issued to that staff member.

xvii. Only Corporation owned or authorized devices or mobile devices may be connected to the Corporation network including the Brock Private WI-FI network. Use of personal devices or mobile devices on the Brock Guest WI-FI Network is permitted but shall be in keeping with the Staff Code of Conduct and security procedures outlined above.

Any security breach or suspected activity as outlined above must be reported to the Department Head and/or Manager of IT. Any incidents, whether deliberate or accidental, will be investigated to determine the severity. All investigation results will be brought forward to the CAO/HR to determine what, if any, actions are to be taken. Depending on the severity of the incident disciplinary measures up to and including dismissal may be considered.

Signature of Staff Member: _____

Signature of Department Head: _____

Date of Completion: _____