TOWNSHIP OF SOUTHGATE
Policy # 83
Information Technology (IT)
& Mobile Device Policy
Approved by Council on: Dec 18, 2019

Information Technology (IT) & Mobile Devices

Purpose

The purpose of this policy is to outline the acceptable use of information systems and computing equipment at The Township of Southgate. These rules are in place to protect Council members, employees and the Township of Southgate. Inappropriate use exposes the Township of Southgate to risks including malware attacks, compromise of network systems and services, loss of confidential information, and legal issues.

Scope of Policy

This policy applies to all Township of Southgate devices, employees and contractors. All employees and contractors with access to Township of Southgate computing devices or information systems shall comply with this policy as it applies to their job duties.

Definitions:

Protected Information: Information that is highly sensitive and that must be safeguarded in accordance with legislative or regulatory requirements. Protected Information is often subject to privacy breach notification laws, and the loss of this information could have severe consequences for the organization. Examples include Protected Health Information, Payment Card Information and most forms of Personally Identifiable Information (PII).

PII (Personally Identifiable Information): Defined in NIST Special Publication 800-122 as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Confidential Information: Information owned by the organization or entrusted to the organization that is not intended for sharing with the public. Security protections must be applied to this information to safeguard its confidentiality, integrity and availability.

Mobile Phones: Any portable phone device (smart or otherwise) that, in addition to having the capability to make and receive phone calls, is also capable of receiving, transmitting and/or storing confidential information.

External Storage Devices: Any device that connects to an external interface of a computer, or to which data can be transferred. This including, but is not limited to USB, eSata, Firewire, Bluetooth, and wireless devices.

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

Public Networks: Any network that is located in a public location and allows patrons, customers, or other, non-authenticated users to connect to the network.

Acceptable Use

General and Internet Use

Employees and contractors shall not, under any circumstances, use Township of Southgate computing devices or information systems to:

1. Engage in any activity that is illegal or violates the rights of any person.
2. Download or install software of any type without authorization.
3. Copy or distribute any copyrighted material without authorization.
4. Access the personal information of others without authorization, except as part of the employee's or associate's assigned duties.
5. Make any claims on behalf of the Township of Southgate unless authorized to do so.
6. Associate the Township of Southgate's name with any activity that would harm the reputation of the organization.
7. Visit websites exhibiting sexually explicit material, gambling sites or sites related to illegal activities.
8. Visit websites that encourage discrimination or the violation of the rights of any group or individual, except in the course of authorized research.
9. Visit websites which share music or other files on a peer-to-peer basis, or otherwise share content in violation of copyright laws.
10. Engage in any activity that interferes with the ability of another organization or individual to conduct computing activities (e.g. denial of service attacks).
11. Provide information about the Township of Southgate or its employees, clients, customers, patients, or associates to any outside party, unless explicitly authorized to do so.
12. Post comments or other information to social networking sites or blogs on behalf of, or using the name of the organization, unless explicitly authorized to do so.

Personal Internet Use

Access to the Internet has been provided as business tools for employees to assist them in performing their responsibilities. Activities of a personal nature such as non-business online shopping, access to personal email and access to personal pages of social networking sites are permitted outside of business hours, provided that all other usage policies are adhered to.

Online File Sharing, Transmission and Storage

Online file sharing, transmission and storage of data using tools such as Dropbox, Google Drive, OneDrive, etc. are very convenient ways to store and share files online but increase the risk that Confidential Information or Protected Information will be inappropriately shared. The following controls must be followed:

1. Information must not be copied to or stored on any online file sharing or backup system without specific authorization from the Township's third party I.T. support.
2. Employees and contractors must not transmit any Protected Information in any email or via any instant messaging or chat service.
3. All Protected information must be transmitted via a secure file transfer method.

4. All Protected Information shall be processed and stored within the applications authorized by the organization. No employee or contractor may copy any Protected Information to any other location unless directed to do so by an authorized Township of Southgate representative.

Email Usage

Email is an important communication tool, but also has the potential to cause damage to the organization. Inappropriate use of email can result in the loss of sensitive or company confidential data or intellectual property, damage to public image, damage to critical internal systems, and unintentional employee exposure to inappropriate content or material.
Township of Southgate employees and contractors must not engage in any of the following:

1. Sending unsolicited email messages, including sending "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Harassment in any form, whether through language, frequency, or size of messages.
3. Creating or forwarding "chain letters" or "Ponzi" or other "pyramid" schemes of any type.
4. Sending similar email messages from multiple email addresses with the intent to harass or elicit replies.
5. Using unsolicited email originating from within the organization's networks or other Internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by the organization.
6. Posting the same or similar non-business-related messages to large numbers of internet posting sites.
7. Unauthorized use, or forging, of email header information.

Social Media

Social media sites are places on the internet where people can share information, interact and communicate with each other (e.g. Facebook, LinkedIn, and Twitter). Social media can be a valuable tool for the promotion of the organization, its goals, and its values. It can also be used as a means of sharing valuable information for the purpose of helping others improve security and reduce risk. However, messages posted to social media sites must be carefully considered, because once posted, these messages cannot be recalled or removed easily, if at all.
No employee or contractor shall post to any social media site on behalf of the organization or claim to represent the organization in any way, without authorization.

All employees and contractors who are authorized to post to social media sites on behalf of the organization must adhere to the following standards:

1. Be respectful of the organization, as well as its employees and associates. Do not post derogatory, malicious, demeaning, insulting or inflammatory comments about anyone or any organization.
2. Use the first person (I, not we) and always appropriately identify yourself.
3. Be accurate.
4. Cite source material. If you have obtained information from an online or other resource, cite the source. If possible, cite the original source. If you are stating an opinion, rather than a fact, make sure this is clearly represented.
5. Clearly state that your opinions are your own, and that they are not the official opinions of the Township of Southgate.
6. Do not use profanity, ethnic slurs or abusive language.
7. If you make an error regarding facts, post a correction or retraction as soon as possible.
8. Protect confidential and proprietary information. Do not identify coworkers, customers, business partners or suppliers without permission.
9. Do not use copyrights, trademarks, or logos without permission.

10. Be professional. Any blog or social media posting that mentions or can be associated with the Township of Southgate becomes a part of the organization's public image. Restrict your comments to those subjects about which you have knowledge. Make sure your posts are making a positive contribution to both the organization's image and to your personal image as an employee or contractor.

Remote Access and Personal Wireless Networks

1. No employee or contractor is permitted to install any wireless networking device that connects to the organization's systems without authorization from the IT administrator, or other appropriate party.
2. No employee or contractor may install any software or application that allows access to the organization's systems from a remote location without appropriate authorization from the Township of Southgate.

Reporting Security Incidents

All employees and contractors must report the following as security incidents to a department head or the CAO:

1. Any observed unauthorized disclosure of Protected Information or Confidential Information, whether intentional or unintentional.
2. Any observed attempt to view or access Protected Information or Confidential Information beyond by a person not authorized to view or access that information.
3. Any unauthorized attempt to gain physical access to, or install unauthorized software applications on, any server or workstation.
4. Any telephone, email, or other communication that include an unauthorized attempt to receive or access Protected Information or Confidential Information.

If any unusual computer behavior (unusual error messages, unusual pop-up windows, website redirection, etc.) occurs, contact the Township of Southgate's third party I.T. support immediately.

Protecting the Organization from Cyber Threats

Sooner or later the Township will be the target of an attempt to trick an employee or contractor into disclosing Protected Information or Confidential Information or installing malicious software on Township of Southgate's systems. Be aware that cyber-criminals often conduct extensive research in preparation for their attacks and may present you with names, events, or other information that you would not expect to be known to anyone outside your organization. Be aware of the following considerations:

1. Exercise caution with email attachments and links in email messages. If the message is unexpected or if you have any doubt about whether it is genuine, contact the sender. Do not reply to the email. Contact the sender using contact information you have previously recorded.
2. Be suspicious if anyone asks you for a password, account information, or other confidential information. Phishing email messages can be made to look exactly like legitimate messages you have received in the past.
3. Never send Protected Information or Confidential Information, enter passwords, or provide account information over an insecure connection. A secure connection will always start with https:// in the browser address bar.
4. Do not click on banner ads or the ads along the top, sides, or bottoms of web pages. These ads are designed to be tempting, but some may link to malicious websites.
5. Understand that you will be targeted by cyber-criminals and that they want to steal confidential information from all businesses, both large and small. Be constantly vigilant.

Remote and Mobile Computing

Remote Information Processing refers to performing information processing activities in a remote location other than a Township of Southgate controlled facility. It includes the following sites:

1. Fixed locations (such as a residence)
2. Mobile locations (such as a hotel or airport)
3. Third-party locations (such as business partners or contractor agencies)

Mobile Devices
Mobile computing devices include any computing device or media that is easily transportable outside of Township of Southgate premises, such as but not limited to the following:

- Laptop computers
- USB mass storage devices
- Mobile phones
- External hard drives
- Optical media (CD/DVD/Blu-ray)

Accidental loss or theft incurs numerous hard and soft costs including the following:

- Replacement cost of hardware
- Re-licensing of software (operating systems/applications)
- Incident reporting
- Lost productivity
- Exposure of proprietary information
- Exposure of sensitive employee information
- Exposure of sensitive or confidential customer information
- Potential federal, state and local fines associated with exposure of confidential employee or customer information
- Damage to the reputation of the Township of Southgate
- Misuse of Township of Southgate's resources (for example, to commit a crime or harass the Township's Users/customers)
- Risk to Township of Southgate networks due to access to remote dialup scripts, email addresses, and passwords

Mobile Phone Usage
Only Township of Southgate mobile phones are permitted for conducting business requiring the use of a mobile phone. The use of a personal mobile phone for conducting Township of Southgate business is prohibited unless the use of a personal mobile phone has been approved by the Township of Southgate staff management.

General Provisions

All Township of Southgate computer equipment security requirements are in effect including mobile phones and devices. These requirements include, but are not limited to:

1. Strong authentication using password, PIN and/or biometric security;
2. Prohibition of installing unauthorized software;
3. Prohibition of modifying configuration settings;
4. Report a lost or stolen mobile phone immediately;
5. Keep your mobile phone in a secure location when not in use and never leave it unattended;
6. Lock the device with a password or Personal Identification Number (PIN);
7. Install Apps only from trusted sources;

8. Back up your data;
9. Keep your system updated;
10. Do not change your security setting or Internet Protocol (IP) address(es) on your device;
11. Remember to log out of banking and shopping sites;
12. Turn off Wi-Fi and Bluetooth services when not in use;
13. Avoid sending personal information via Text or Email;
14. Be careful what you click;
15. Do not send confidential data over insecure (HTTP) connections; and
16. Do not connect to company resources from public networks (coffee shops, restaurants, libraries, airports, etc.).