

PROTECTING YOUR Municipality FROM CYBER THREATS

The threat to your information, and the computer systems that process that information is at an all-time high. While everyone is at risk, the impact to organizations that operate time-critical or emergency services such as municipalities can be particularly significant.



Identify Critical Systems

Create a list of all of the major functions performed by your municipality, and then rank them based on importance. For each function, identify the computing systems that support the function; these are your critical systems.



Take a Data Inventory

You cannot hope to protect your data if you do not know what you have or where it is stored. Identify all of the physical and virtual locations where you collect, process, or store data. Once you have a complete list, identify the types of data at each location (i.e. financial, personnel, health, etc), if it is necessary to collect and retain, and how it is to be protected.



Back It Up

Create regular backup copies of your data and store them offline (i.e. on DVD, tape, external hard drive, etc) at a geographically separate location. Storing backups at an offsite location helps protect the data against physical disasters like fire and puts it beyond reach of threats such as ransomware. How often backups occur depends on the data; financial transactions may need to be backed up nightly, while other records may be weekly or monthly.



Create a Continuity Plan

Do you know how your municipality's emergency services, infrastructure, or employee payroll will function in the event you have no computer systems or telephone capabilities? Develop a business continuity plan that outlines in detail how your critical infrastructure and services will maintain operations during the loss of power, communications, or computing capabilities.



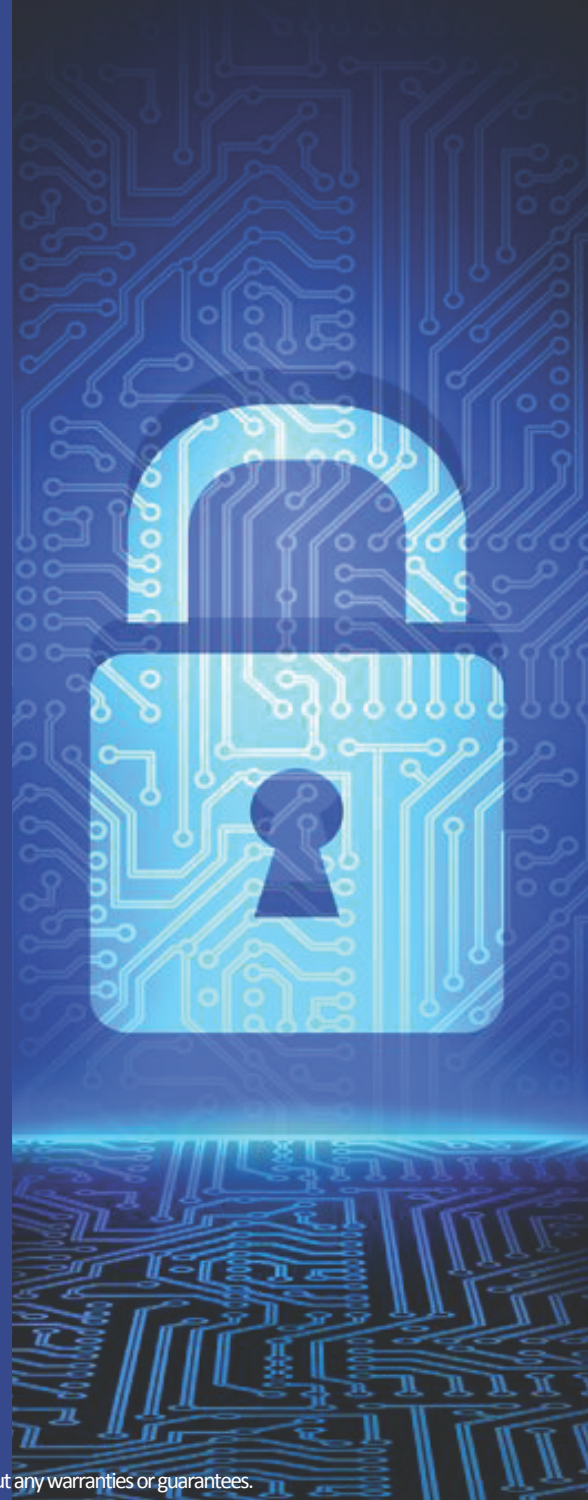
Actively Manage Your Risk

Implement a risk management process, such as the National Institute of Standards and Technology (NIST) Risk Management Framework, to ensure you identify and appropriately address risks to your information systems. For more information visit <https://csrc.nist.gov/>



Educate Employees

People are an important component of every information system. Educate your employees on how to identify and respond to common cyber threats, and enforce good habits such as proper password management. For more information visit <https://staysafeonline.org/>



The information and opinions contained in this document are provided "as is" and without any warranties or guarantees.