Published on *Vermont League of Cities and Towns* (https://www.vlct.org)

Techology Assessments - Learn About Your Systems

How do you know if your computer systems or physical office space is at risk for cybersecurity threats and intrusions? Before throwing up your hands and hiring a vendor, you can use lots of free resources designed to help anyone from novices to experts better understand their technological footprint. You don't need any special training or knowledge to be proactive today. We have compiled a few resources to help you get started. Approach this as an internal audit to learn about your systems. There are checklists available online that mimic those used by technology and cybersecurity firms. For more information on security audits as well as technology and cybersecurity services, view the links at the bottom of this page.

The first step is to inventory your municipality's digital and paper assets. This includes systems and hardware used by officials who conduct business outside the town office (such as individuals who send town-related emails from personal email accounts using his or her home computer).

General Asset Sample Inventory Questions

1. What kinds of records do you manage?
2. What format are they in?
3. How are they stored?
4. What software and hardware are you using?
5. What digital security measures are you currently aware of that are in place? (examples include: virus software, password managers, multi-factor authentication, etc.)
6. How is your physical workspace set up? What kinds of security do you have in place for physical assets? (sign in sheets for visitors, key cards, video cameras, etc.
7. Who has access to your systems, office space, and passwords?
8. Do you have a technology use/cybersecurity policy? Is it up to date
9. How often, if ever, do you or your staff receive training? Who conducts it? What topics?

Review the guidance, checklists, and samples via the links below to customize your own assessment.

Understanding your systems will help you better assess the security currently in place as well as what may be needed. Next, identify questions you have about those systems and assets to share with internal staff or vendors responsible for you municipality's technology security. We have provided a list of resources below to help you in start this process.

Conducting an internal audit prior to engaging an IT service provider or with your current vendor can be helpful: check out the VLCT Information Technology Audit - Learn About Your Risk resource below for some vendor information, useful tools and guidance on conducting an IT audit.

Links:
* VT Goverment Finance Officers Association Technology Needs Asesment Manual [1]
* US Department of Homeland Security Cyber Resilience Assessments & Guidance [2]
* Office of the New York State Comptroller Information Technology Governance Manual [3]
* State of Massachusetts IT Best Practices Guide for Small Municipalities [4]
* National Institute of Standards and Technology Risk Management Framework for Information Systems and Organizations [5]
*VLCT Resource Page IT Security Audits - Learn About Your Risk [6]
*Back VLCT Cybersecurity Page [7]

Publication Date:
Friday, March 01, 2019

Resource Category:

- Guidance

Links
[1] http://www.gfoa.org/sites/default/files/TechnologyNeedsAssessments.pd
[2] https://www.us-cert.gov/ccubedvp/assessments
[3] https://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf
[4] https://www.mass.gov/files/documents/2018/02/09/IT%20Best%20Practices%20Guide%20for%20small%20munis%20and%20Conway.pdf
[5] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
[6] https://www.vlct.org/node/11272
[7] https://www.vlct.org/municipal-assistance/cybersecurity