Cybersecurity

Cybersecurity and proper technology use are paramount concerns for all manner of business and governmental entities. Organizations that maintain large stores of personally identifiable information (PII), such as social security numbers, financial information, personnel records, and the like, are at significant risk of security breaches, internet scams, and ransomware (malicious software that blocks access to a computer system until a sum of money is paid) threats.

In response to member requests and concerns, VLCT now provides cybersecurity-related guidance, resources, training, and support for members.

This webpage includes links to online resources as well as announcements of assistance and training offered by VLCT and PACIF. Follow the links for internal and external resources available to assist small and large municipalities in developing and improving upon their security measures. You don’t need special training or expertise to take steps today! Check the Resources list below for more information.

Members, please feel free to contact us at 1-800-649-7915 or info@vlct.org [1] if you have ideas about how VLCT can assist with your technology efforts.

Cybersecurity Vendors - Security Audits

VLCT has compiled a list of several IT service providers and security firms [2] interested in offering cybersecurity audits to local governments. Please note that this is not an exhaustive list, VLCT has not vetted these organizations, and we do not endorse any particular business entity at this time.

In the Resources list below you will find links to external resources on vetting security and IT service providers, questions to ask when selecting a provider, information on how to conduct an internal technology assessment, and audit checklists to get you started.

If you are a vendor and would like to be included on future updates, please contact VLCT.
Links
[1] mailto:info@vlct.org