LGC's Cybersecurity Services

Local Government Corporation (LGC) offers a wide range of Cybersecurity services to better secure customer data including antivirus software, a cloud-based and local backup solution, advanced monitoring, and detection software, as well as multi-factor authentication. Detailed information regarding these services is listed below including how they help protect against cyberattacks and LGC's response should a breach occur.

Cyber plan suggestions and cybersecurity guidelines can be found on the Tennessee Comptroller's website at:
https://comptroller.tn.gov/office-functions/la/resources/cyberaware.html.

Antivirus

- **Protection**
  LGC's cloud-based, business class antivirus software helps detect, prevent, scan, and delete malware (malicious software) and viruses. The software runs automatically in the background to provide protection against virus attacks. It is comprehensive virus protection to help protect files and hardware from malware such as worms, Trojan horses, and spyware. LGC's antivirus software includes an auto-clean feature that deletes harmful software, automatic update for new types of malwares, protection against multiple types of malwares across multiple applications, and scanning for the presence of malware.
- **Response**
  Once contacted by the customer regarding the concern of an infection, LGC will investigate. If LGC determines there is an infection, then the computer would be cleaned of the virus or reloaded if necessary.

Backups (Local & Cloud)

- **Protection**
  LGC's One Backup combines local and online backups into a single product. All the details of the backups are available in an easy-to-read interface, including when an individual file was last backed up or the status of the backups. Restoring a file or folder is just as simple as locating a file in Windows. LGC monitors the backups to confirm the Cloud as well as local media (SSD Drives/Thumb Drives) backups were successful. Once

per year, LGC will download a Cloud backup of LGC's software to verify that it is valid and send a letter to the customer upon completion.

- **Response**
  Multiple versions of the customers files are backed up daily. In the event the most recent version of the backup is encrypted or corrupted, LGC can easily restore an earlier version. Cloud backup storage cannot be modified from the user side, so backups cannot be removed.

Fortress

- **Protection**
  Fortress provides real-time visibility of suspicious/malicious behavior. It uses an advanced monitoring and detection method that helps identify a broad range of attacks and helps prevent such activity instead of just reacting to the all too real consequences. This service allows LGC to react in real-time and provide notification of attacks and assist in blocking those intrusions as well as assisting in operating system and program updates, which help maintain overall computer and system health. Fortress helps protect against ransomware by detecting an encryption event before it does damage. LGC will monitor the behavior (processes in use, programs installed, and sites visited) of an endpoint (server & workstation) and will assist with audit or insurance questionnaires.
- **Response**
  If suspicious activity is detected, Fortress stops the process and quarantines the files. If the activity is determined to be a false positive, the files can be restored. Fortress also provides information on the process and files involved for investigating the incident.

  Fortress ensures the Windows operating system and third-party software updates are applied. Windows operating system updates are one of the most important things customers can do to keep computers safe from new vulnerabilities. Fortress also keeps the systems running like they should by checking the Windows logs and alerting LGC of any issues with the operating system or hardware.

  LGC monitors devices with Fortress installed to ensure the Windows operating system and other updates have been applied and reboots the computers if necessary. If any operating system or hardware issues are detected, LGC alerts the administrator of the device and provides details on the issue.

Sentry

- **Protection**
  Sentry is LGC's multi-factor authentication (MFA) service. It is powered by industry leader, Duo Security. MFA requires two or more verification factors to log into an account. MFA is a core component of a strong identity and access security policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyberattack. Verifying identity using a second factor (such as a phone or other mobile device) prevents anyone else from logging in, even if they know the password. Sentry adds a second layer of security, helping to keep accounts secure even if a password has been compromised. Sentry is easy-to-use with real-time identity authentication via fast push notifications, and it helps meet cyber insurance carrier requirements.
- **Response**
  Sentry protects the user's Windows login, so they are aware of any login attempts to their account. Even if their Windows password is compromised, the user will still have to approve the Windows login with their mobile device. Any outside intrusion attempts would have to be approved by the user.