Local Government Corporation
Cybersecurity Information Guide

This document is being provided for the purpose of assisting our customers with responding to questions regarding cybersecurity that may be asked during an audit. However, it is not intended to provide a detailed analysis and review of all components that make up a system. Due to the wide variety of computers, operating systems, network components, and peripherals of varying age that exist at LGC customer offices, the answers provided below primarily address systems that were purchased directly from LGC and are not obsolete due to age or OEM retirement. Systems that are obsolete or purchased/maintained by a provider other than LGC are not addressed in the responses below. Additionally, these responses are general in nature, therefore, variances at individual customer offices are likely.

- How are operating system updates applied to workstations and servers? Are these updates installed automatically or on a set schedule so that all current updates are installed timely?
    - During installation, all computers purchased from LGC are set to automatically update weekly and apply updates for all Microsoft products and drivers.
    - Additionally, LGC offers an optional managed network service to monitor the customer's LGC servers to ensure all critical updates are verified and applied in a timely manner.

- Are software and database patches applied to accounting software?
    - SQL updates are applied through windows updates.
    - Software updates are automatically applied to LGC cloud hosted software and the TnCIS software. Software updates are made available to customers for download for all other LGC on premise software.

- Do the workstations and servers have antivirus software installed? Is this software configured to receive definition updates automatically? How often does it run a scan to detect malicious software?
    - LGC recommends antivirus software for all computers purchased through LGC. If the customer chooses to purchase antivirus software, it is configured to scan periodically for threats and automatically apply any manufacturer updates as they become available. LGC also offers Malwarebytes software that scans for malicious malware.
    - Additionally, LGC offers an optional managed network service where antivirus software and Malwarebytes are managed by LGC and verified periodically.

- If wireless networks are used, do they use encryption? Has the password for the devices used (routers, access points, etc.) been changed from the default password assigned by the manufacturer? Is the network name (SSID) hidden?
    - At time of installation all wireless devices installed by LGC has at least WPA2 encryption enabled and the network passwords are given to the customer. We also set the admin username and password that does not include any of the default manufacturer passwords. LGC recommends the SSID be hidden.

- Are firewalls used? If so, what product is used and is it configured to limit access to your network? Are logs reviewed?
    - LGC currently offers a Cisco RV340 for customers needing a firewall. As part of our optional Network Services Managed Service, LGC also offers an LGC EDGE firewall device. Both devices are configured to only allow traffic into the network per customers' needs. Both devices we offer have logging functionality. Upon request by the customer, non-network managed sites will have logging turned on. As part of our optional Network Services Managed Service, LGC reviews the logs for those customers.

- Do you allow remote access to your system via VPN, remote desktop software, or other means? What product is used and how is it secured?
    - LGC will configure remote access only upon request by the customer. LGC offers both VPN and remote connection software. Each have 256-bit encryption plus password complexity to help secure the connections.

- Do you ever perform vulnerability scans of the network?
    - Upon request, LGC may perform a vulnerability scan when asked for a specific reason.
    - This service is routinely performed and included as part of our optional Network Services Managed Service.

- Does the backup process capture all data vital to the operation of the office? In addition to the accounting system, are other critical files such as spreadsheets and documents backed up?
    - At time of installation, LGC configures the backup to capture all critical data pertaining to the LGC software along with any data on the L drive and other folders specified by the customer.

- If the office were to fall victim to a ransomware attack, is the backup process configured so that backup data would not be encrypted in the attack?
    - LGC recommends a daily backup performed on separate media for each day of the week Monday-Thursday, along with two separate media for Friday which are rotated off site weekly. The media contain three weeks of backups. Additionally, an optional online backup service is offered (LGC One Backup) that backs up every four hours resulting in approximately 85 separate backups over a two-week period.

- Are there any other measures in place to protect the office from a cyberattack?
    - Several times throughout the year LGC communicates with our customers the importance of backups, offsite and cloud backups, antivirus and malware software and the importance of keeping all hardware current and updated.