IT Asset Protection Checklist

- [ ] Are staff required to complete security awareness training during the on-boarding process, as well as annually?
- [ ] Does the organization have a system to track IT assets?
- [ ] Does the organization encrypt all hard drives?
- [ ] Are staff local administrators on their devices?
- [ ] Is there a list of approved applications for devices?
- [ ] Are staff required to have a secure pin/password for their mobile device?
- [ ] Does the organization require two factor authentication or multi-factor authentication?
- [ ] Do staff know who to inform that a breach occurred?
- [ ] Does staff know if management has the right to access their corporate devices?
- [ ] Does the organization have a password policy?
- [ ] Does the organization have a backup and recovery policy? Does staff know how often files are backed up and how long they are accessible? Are backups tested regularly?
- [ ] Does the organization have a computer acceptable use policy? Does staff acknowledge and understand the policy?
- [ ] Is there a remote access policy? Are all staff permitted to work remotely? Are there additional security measures applied when connecting to the network remotely? (i.e. multi-factor authentication)
- [ ] Does the organization have a patching policy?
- [ ] Does your organization have a Business continuity plan? Is it tested regularly?

For more information about IT risk, visit our website at www.grfcpa.com/accounting-services/advisory-services/cybersecurity-and-it-risk/.