HOSPITALITYLAWYER.COM®

Terms and Conditions for Forms, Checklists, and Procedures

Forms, checklists, and procedures at HospitalityLawyer.com are provided as informational, educational, and illustrative purposes only. HospitalityLawyer.com does not render legal advice. You should always consult legal professionals for your specific needs, questions, and services. If you choose to use a form, checklist, or procedure, you do so at your own risk. HospitalityLawyer.com does not make any representations that the forms, checklists, or procedures are suitable for a particular use and the user should always independently assure themselves of the accuracy and legal compliance for their particular jurisdiction.

CYBERSECURITY CHECKLIST

TRAIN YOUR STAFF

- [ ] When onboarding new hires, include cybersecurity awareness training and promote cybersecurity best practices. Encourage employees to utilize their training to protect their personal data and devices in order to develop greater consistency in their cyber defenses.

- [ ] Maintain regular re-training and evaluation sessions for experienced staff. Without frequent cybersecurity compliance training or genuine cyber breach incidents, it can be easy for employees to develop a false sense of security.

SECURITY & RISK ASSESSMENTS

- [ ] Review your security and perform risk assessments regularly. A full review and assessment should be conducted annually, at minimum, but quarterly reviews are recommended. Further reviews and assessments should be conducted if a new technology or vendor is acquired.

- [ ] Review and assess the cybersecurity practices for current as well as potential vendors and service providers. Be sure to fully understand how a vendor or service provider will interact with your organization's system(s) and data.

- [ ] Ensure that your system(s) and software programs are updated regularly. Missing out on an update can lead to weak spots and greater vulnerability.

SYSTEM SET-UP & MANAGEMENT

- [ ] Identify the specific requirements for your organization. The best cybersecurity awareness training will be customized to best fit your organization's needs and wants.

- [ ] Familiarize yourself (and staff) with the technology and systems used by your organization and know what data is collected. Understand how different devices and systems work, both jointly and individually, and what vulnerabilities they...

CYBERSECURITY CHECKLIST

...may already have and develop in the future. Be sure to keep yourself (and staff) updated on any changes to existing or newly acquired systems, devices, software, or vendors/service providers.

- [ ] Keep Wi-Fi networks secure and separate. Maintaining one Wi-Fi network for guests and visitors and another for your organization's business is ideal. A robust security software program on all computers and devices is also recommended.

- [ ] Use tokenization and/or encryption to keep data secure. Tokenization will remove data from a system and replace it with an associated value. Encryption leaves the original data (such as credit card information) intact but makes it inaccessible without a proper key. Tokenization removes the data from a system entirely and replaces it with a randomly generated non-sensitive placeholder (or a token).