Brokerage Cybersecurity Checklist

INFORMATION SECURITY PROGRAM	Yes	No
Does your brokerage currently have a cybersecurity plan (or program)?	□	□
Do you use information security practices in your brokerage operations?	□	□
Do you have policies around user authentication, authorization, and access to sensitive information?	□	□
Have you documented your information security policies and procedures?	□	□
Do you have information security compliance standards and controls included in your information policies and procedures?	□	□
Have you set enterprise risk management procedures to identify, assess, control, and review risks within your brokerage?	□	□
Do you have a cybersecurity strategy, including plans to minimize risks?	□	□
Do you have control systems in place to prevent and detect unauthorized access to sensitive information?	□	□
INFORMATION SECURITY OPERATIONS	Yes	No
Do you protect sensitive information by encrypting computers, mobiles devices, and backup storage?	□	□
Do you restrict the sharing of personal or sensitive information over unencrypted public networks?	□	□
Do you restrict access to the physical servers that contain or process sensitive information?	□	□
Do you only allow a user to access and make changes to systems and data based on their job function?	□	□
Do you restrict access to computers systems to authorized personnel only?	□	□
Do you limit the use of software on brokerage computers to an approved software list?	□	□
Does your computer equipment, that stores or processes sensitive information, automatically lock after a set time limit for inactivity?	□	□
Do you install and regularly update endpoint protection software, antivirus software, and antimalware systems?	□	□
Do you regularly update software applications, operating systems, servers, and networking systems?	□	□
Do you perform regular security audits (or vulnerability scans) on your servers, network equipment, and computer systems?	□	□
Do you restrict software installation to authorized IT staff?	□	□
Do you enforce the use of secure passwords?	□	□
Have you implemented Multi-Factor Authentication (MFA) technology for accessing sensitive information remotely?	□	□
INFORMATION MANAGEMENT	Yes	No
Do you identify, classify, and protect sensitive data?	□	□
Do you encrypt valuable or sensitive data based on classification?	□	□
Do you have policies and procedures for:	□	□
• handling credit card information?	□	□
• handling personally identifiable information?	□	□
• disposing of or destroying sensitive information?	□	□
• the backup and archival of critical information?	□	□
Do your securely wipe all devices before they are repurposed or discarded?	□	□

INCIDENT RESPONSE PLANS AND BUSINESS CONTINUITY	Yes	No
Do you have an up-to-date business continuity plan?	□	□
Do you have an insurance policy to mitigate a cybersecurity breach?	□	□
Have you the documented process for responding to a suspected breach?	□	□
Have you trained employees on the process?	□	□
Do you have an up-to-date emergency evacuation plan?	□	□
Does this plan identify the areas that need to be sealed off immediately in case of an emergency?	□	□
Are key personnel trained regarding this?	□	□
Do you have a process for regular backups and a plan to access archival data in the event of a disaster?	□	□
Do you have an emergency/incident management communications plan?	□	□
Does your plan set procedures for notifying the relevant authorities in the case of a disaster or security incident?	□	□
Do your procedures identify who should be contacted for each type of incident?	□	□
Do your procedures identify the person authorized to make this contact?	□	□
Does your plan identify who is authorized to speak to the press/public in the case of an emergency or an incident?	□	□
Does your plan set procedures for internal communications with your employees and their families?	□	□
Can your emergency procedures be appropriately carried out, as needed, by the people responsible?	□	□

SECURITY AWARENESS AND EDUCATION	Yes	No
Do you provide information on cybersecurity to your staff?	□	□
Do you provide your staff with regular cybersecurity training?	□	□
Do you train your employees to be alert to possible security breaches?	□	□
Do you have software installed to protect employees from online and email threats, including malware, phishing, and spam?	□	□
Are your employees trained to identify and protect classified data, including data stored:	□	□
• in hardcopy?	□	□
• electronically, on shared networks?	□	□
• electronically, on removable media (e.g. USB drives, laptops, etc)?	□	□
Do you provide training on how to properly handle sensitive information such as credit card data and personal private information?	□	□
Do you perform regular mock phishing campaigns to help train your employees to identify phishing techniques and methods?	□	□

COMPLIANCE AND AUDIT	Yes	No
Do you regularly review and revise your information security policies, standards, procedures, and guidelines?	□	□
Do you perform regular security audits to ensure unauthorized software applications are not installed?	□	□
Do you monitor, log, and report all intrusions?	□	□
Do you perform regular tests on your security systems to check for vulnerabilities breaches or attacks?	□	□
Do you update your security systems when testing indicates they are vulnerable?	□	□