ProCircular
SECURITY. PRIVACY. TRUST.

2451 Oakdale Blvd.
Coralville, IA 52241
844-95-SECUR
www.procircular.com

Cyber Insurance Baseline Analysis

1. Does the Applicant use multi-factor authentication ("MFA") for all remote access to the Applicant's computer network?
2. Does the Applicant download, test, and install security patches within 30 days of release onto the Applicant's computer network (including all hardware and software publicly accessible through the internet)?
3. Are all systems and data on the Applicant's computer network backed up at least weekly?
4. Are the Applicant's backups kept fully isolated from the Applicant's computer network, either in:
    A. Offline air-gapped storage; or
    B. Cloud-based storage, so that the Applicant's backups are isolated from the rest of the Applicant's computer network before and after back-ups are completed?
5. Does the Applicant exclusively run supported operating systems on the Applicant's computer network?
6. Does the Applicant scan and filter incoming emails for malicious attachments?
7. Does the Applicant use any of the following to authenticate incoming email?
    A. DomainKeysIdentified Mail ("DKIM"); or
    B. Sender Policy Framework ("SPF"); or
    C. Domain-based Message Authentication, Reporting & Conformance ("DMARC").
8. Has the Applicant disabled the Remote Desktop Protocol ("RDP") on all computer network endpoints and servers?
9. Does the Applicant encrypt all sensitive and confidential information stored on the Applicant's computer network and while in transit?
10. Are administrative privileges restricted to specific users on the Applicant's computer network?
11. Does the Applicant have policies and procedures for cybersecurity awareness education and training of employees to properly handle funds transfers?