TDI | Texas Department of Insurance

Evaluation of enterprise risk

Confidential cybersecurity checklist

► Section 1: Names of legal entities

Name of your holding company system:

_____

Names of any legal entities not included in the responses below:

_____

Explain why you excluded those entities:

_____

► Section 2: Answer yes or no and provide comments below if response is "no":

1. When did you last perform a thorough research on all the operating systems, Software applications, and data center equipment used by the holding company system? Enter date performed: _____ ☐ Yes ☐ No
2. When did you last review the IT policies and procedures used by the holding company system? Enter date performed: _____ ☐ Yes ☐ No
3. Do you have a cybersecurity incident response plan in place? ☐ Yes ☐ No
4. Do you have a set of predefined communication guidelines that can be used in the event of security failure? ☐ Yes ☐ No
5. Does your holding company system have appropriate back up procedures in place to minimize downtime and prevent loss of important data? ☐ Yes ☐ No
6. Is there a cybersecurity training program in place for current and new employees? ☐ Yes ☐ No
7. Do you restrict administrative and privileged access to systems and data through preventative and detective controls to prevent unauthorized access or alteration of systems and/or data? ☐ Yes ☐ No
8. Do you allow only trusted software to execute on operations systems? ☐ Yes ☐ No
9. Do you prevent the execution of other than trusted software through the use of application whitelists? ☐ Yes ☐ No
10. Do you have a patch management application for both your servers and every computer and workstation used in your holding company system? ☐ Yes ☐ No
11. Do you have antivirus installed on your servers and on every computer and workstation used in your holding company system? ☐ Yes ☐ No

12. Does your holding company system have a host intrusion prevention solution or a firewall installed? ☐ Yes ☐ No
13. Do you periodically perform vulnerability scans on your servers and all the computers and workstations used in your holding company system? ☐ Yes ☐ No
14. Do you use local encryption solutions for every computer and workstation, including mobile devices, used in your holding company system? ☐ Yes ☐ No
15. Do you employ a password management system for every user in the holding company system? ☐ Yes ☐ No
16. Do you enforce robust password security per NIST standards that include:
    - Upper and lowercase letters, numbers, and symbols ☐ Yes ☐ No
    - A minimum of eight characters, avoiding common words and dates ☐ Yes ☐ No
    - A dedicated password (one not used for any other credential) ☐ Yes ☐ No
    - Regularly changed passwords ☐ Yes ☐ No
    - Multi-factor authentication ☐ Yes ☐ No
17. Do you have email filtering and internet traffic filtering software that protects users from the full range of email threats, including malware, phishing and spam? ☐ Yes ☐ No
18. Does your holding company system have a long-term plan concerning its cybersecurity strategy, including plans to mitigate any IT system gaps resulting from merger or acquisition activity? ☐ Yes ☐ No

If you answered "no" to any question in Section 2, state the reason below:

Item number and reason:

_____

_____