BOXTOP CYBERSECURITY EXECUTIVE SUMMARY

Tabush Consulting Group Inc. & Tabush Boxtop LLC (Boxtop) employ administrative, physical, and technical safeguards to protect its information. Boxtop's cybersecurity infrastructure was modeled after such industry best practices as the NIST Cybersecurity Framework, NIST Special Publication 800-53, and 20 CIS Critical Security Controls. As such, Boxtop's cybersecurity infrastructure takes into account the requirements of various cybersecurity laws, rules, and regulations including but not limited to the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act. Below is a summary of the types of cybersecurity safeguards Boxtop employs:

PHYSICAL SECURITY CONTROLS

Boxtop uses a number of physical safeguards to protect sensitive information. Access to Boxtop's office is protected by locked doors, alarm systems, cameras, building security, and company policy (employees are instructed to report suspicious activity to Boxtop's Office Manager). Further, Boxtop's servers are located in data centers in the U.S. that employ a number of additional safeguards including but not limited to: security guards that restrict access to the data centers to only authorized individuals, biometric authentication, and logs that identify who physically accessed the servers. Further, the actual servers themselves are stored in locked cages that are only accessible through the use an authorized access card.

Boxtop monitors third parties who may be given access to office and systems. With respect to third-party vendors, Boxtop management and employees regularly manage those relationships. Inconsistencies are investigated and immediately addressed. New staff members sent by third parties are verified with their company before being allowed in.

ADMINISTRATIVE SAFEGUARDS

General Training: New employees at Boxtop undergo a training session with the firm's technology department. Part of this initial training is instruction on the use of computer systems and what to do in the event a security incident (e.g., if a computer begins to act suspiciously). As part of this instruction, employees are educated on common security threats (such as: receiving suspicious emails or file attachments) and how to respond to them, including notifying the technology department immediately. Further, the initial training includes a discussion regarding the protection of confidential information, the prohibition on installing unauthorized software, and following various technical and physical security safeguards. After the initial training, employees are informed of security concerns and safe practices through emails that are sent whenever the technology department determines that a current threat may have the potential to impact Boxtop, and through company-held information security awareness events.

Role Based Training: Members of the IS and IT staff review newsletters, publications, webinars, and online forums regarding new threats.

Background Checks: As part of Boxtop's background check process, Boxtop's human resources department verifies a candidate's references and resume. Further, candidates are usually required to meet with multiple members of Boxtop's management before being hired. For candidates whose position could pose a greater risk, Boxtop utilizes an outside agency to run a background check on the candidate.

Assets Are Inventoried: Physical devices, systems, software platforms, and applications are inventoried.

Organizational Communications and Data Flows Are Inventoried: Boxtop created a topology map showing any internal and external connections to information systems.

External Information Systems: Boxtop's sensitive data is only stored on its own data center servers and an alternative storage site. Boxtop utilizes a number of service providers to assist in providing services, but the service providers do not receive direct access to sensitive information. The agreements with these vendors require them to implement appropriate security controls to protect Boxtop's information in accordance with applicable laws and the firm's cybersecurity infrastructure requirements.

Resource Classification: Safeguards are considered according to the resource's relative importance to business objectives, Boxtop's legal and contractual obligations, and Boxtop's risk tolerance.

Cybersecurity Roles and Responsibilities: Boxtop's cybersecurity infrastructure was created and is maintained by its cybersecurity committee. The cybersecurity infrastructure takes into account the various roles and responsibilities of its employees and any third-party providers.

Risk Assessments: Material changes that have the potential to impact Boxtop's cybersecurity infrastructure are reviewed by the cybersecurity committee. Material changes include but are not limited to: installation of new applications, hiring of new vendors, changes to laws, directives, policies, or regulations. Assessing risk takes into account the criticality of the assets exposed, the likelihood of the threat occurring, and the impact the threat could have.

Threat and Vulnerability Intelligence: Boxtop uses various sources to maintain awareness of new and existing threats, including: security and vulnerability alerts, notices and advisories from computer security online forums, newsletters, and various other forms of news media. Boxtop also keeps in contact with selected groups and associations within the cybersecurity community to facilitate ongoing sharing of current security-related information, including threats, vulnerabilities, and incidents.

Board/Executive Involvement: The cybersecurity committee reports material cybersecurity related risks, changes, and developments to Boxtop's Chief Executive Officer, who informs the rest of Boxtop's management.

Vetting and Engaging of Third-Party Service Providers: To have a third-party service provider approved, the service must first be brought to the attention of a member of Boxtop's cybersecurity committee. As part of considering the third-party provider, the committee evaluates what type of information the provider will have access to, the vendor's reputation in the industry, and the types of security controls they have in place. If the provider will be handling sensitive information, the committee may request the provider send additional information regarding its WISP, evidence of its last internal audits, or evidence of their cybersecurity certification, if available. Prior to contracting, Boxtop takes into consideration the impact of relying on the third party and what kind of damage an interruption of that service may cause its business.

Suspicious activity by a third party is investigated by Boxtop. Depending on the type of information the third party has access to, Boxtop may periodically check online for any negative statements about the third party or any complaints of their cybersecurity practices. In addition, third parties are monitored while accessing Boxtop's systems.

Any issues with third-party vendors are logged and followed up on.

Contracting with Third-Party Service Providers: Boxtop contractually binds third-party service providers to handle sensitive information in accordance with its cybersecurity infrastructure. A member of the cybersecurity committee reviews the vendor agreement to ensure the appropriate provisions are contained within the contract. Depending on what type of information the provider will have access to and criticality of the service, the contract will be reviewed to ensure it addresses the following:

- The ownership of the data
- General and specific security requirements and procedures that the service provider must maintain
- The service provider's ongoing compliance with applicable privacy and data security laws
- Boxtop's right to audit the service provider's security procedures and policies
- Boxtop's right to terminate the contract for material breaches and other remedies, for example., indemnification for losses resulting from the service provider's failure to comply with its data security obligations
- Secure destruction or return of the information to Boxtop on the agreement's termination or expiration
- Requirements and procedures if the service provider suspects or experiences a breach or an incident, such as immediately notifying Boxtop
- Each party's responsibility for bearing the costs incurred in responding to and mitigating damages caused by a security breach
- Any restrictions on the location where the data is stored by or on behalf of the service provider, for example, prohibiting transfer outside of the US

Terminating Third-Party Service Providers: Upon terminating a third-party relationship, all physical and digital access is immediately revoked. Other cybersecurity steps, such as requiring data deletion, are pursued. Additional steps may be taken depending on the nature of the service that was provided by the third-party service provider and the reason for the termination of the business relationship.

Development and Test Environments are Separate: Prior to deployment, new systems, devices, and software are tested first separately and then cooperatively to assure functionality. Prior to deployment, controls are put in place to ensure that newly deployed or rebuilt systems are up to desired specifications with regard to interior patch level requirements. The system/ equipment will not be deployed until identified vulnerabilities have been adequately addressed.

TECHNICAL SECURITY CONTROLS

Monitoring: Boxtop monitors for suspicious network activity. When monitoring software detects irregular activity, it will notify the appropriate Boxtop personnel who will analyze and handle the incident.

Access Restrictions and Controls: Boxtop restricts access based on asset criticality and also monitors its systems, as provided above. Boxtop determines which users are provided elevated access controls based on their roles and responsibilities and in line with compliance requirements.

Data in Transit: Boxtop uses a number of methods to protect data in transit. Data is encrypted across the network (including between Boxtop's office and data center). All emails are configured to generally use TLS encryption.

Data at Rest: Information at rest on Boxtop's information systems is encrypted using AES 256 encryption. Accessing information contained on Boxtop's information systems requires either the encryption key or a valid username and password.

Data Destruction: Data that can be deleted by Boxtop is securely destroyed in accordance with Boxtop's obligations and upon reasonable belief the data is no longer required by both Boxtop and its clients. All equipment is securely erased or destroyed before being discarded.

Backups/Contingency Planning: Backups of information are conducted, maintained, and tested periodically. Boxtop utilizes a redundant email continuity system and enterprise backup solution. Boxtop's offsite backups are encrypted. Recovery mechanisms are tested on a weekly basis.

Patching: Patches are generally applied once per month and are thoroughly vetted by a test group before launching company-wide. Patch application may be hastened based on the relative importance of the system and the severity of any suspected vulnerability.

Password/Session Management: Logged in sessions are set to timeout after a set period. Password policies are configured to include: a minimum password length and require various character types. Two-factor authentication is enabled when available.

Vulnerability Testing: Boxtop tests its information systems for known vulnerabilities on a weekly basis. Boxtop remediates legitimate vulnerabilities, when possible, within one day.

Remote Access: Boxtop monitors and controls all methods of remote access (e.g., dial-up, broadband, wireless) to all Boxtop information systems. Secure remote access is strictly required. Third parties given access to Boxtop information systems are monitored throughout the session and the connection is terminated immediately upon noticing any suspicious activity.

Portable Devices: Boxtop systems are configured to not recognize external storage media attached by USB. Unencrypted portable devices are generally not used to transport sensitive information.

Network Configurations: Boxtop employs the principles of least privilege in all of its configurations, including regarding its use of ports, protocols, and services. Boxtop applies this principle to all networking technology including its firewalls, routers, and switches.

Wireless Access: Sensitive information, such as client information stored on Boxtop's information systems, cannot be accessed through Boxtop's wireless network.

Integrity Checking: Boxtop uses commercial solutions to monitor for irregular file changes.

Baseline/Security Configurations: Systems and devices are installed using predetermined configurations that contain appropriate safeguards. Device and software usage is tracked and unauthorized installations are flagged by detection software.

System and Application Lifecycle: Systems and applications are monitored throughout their lifecycle. End of life dates are tracked and appropriate solutions are found and install.