



## DATA SECURITY ADDENDUM

### 1. POLICIES, STANDARDS & PROCEDURES

- 1.1 Elite will maintain the following policies, standards, and procedures designed to protect the security of its Services:
- (i) Procedures to permit only authorized end users to access Services.
  - (ii) Policies requiring that only Elite' personnel who need access for their responsibilities are permitted to access Services if any.
  - (iii) Policies requiring the use of unique user IDs and passwords for end users.
  - (iv) Procedures to cause connections to the Internet to have commercially reasonable security controls, including detection and countermeasures, designed to detect and prevent unauthorized activity.
  - (v) Procedures for the performance of regular vulnerability assessments of critical applications and network components that support Elite' provisioned Services.
  - (vi) Procedures for the use of anti-malware and patch management controls to protect against virus or malware infections and exploitation of security vulnerabilities.
  - (vii) Standards for the use of audit controls that record and monitor activity related to the Services.

### 2. ASSESSMENT QUESTIONNAIRES & SECURITY ASSESSMENTS

- 2.1 Once per 12 sequential calendar months, Customer may request Elite to complete an information security and physical security assessment questionnaire. Elite agrees to respond to such questionnaire as soon as commercially reasonable.
- 2.2 Upon Customer's request, Customer may review certificates or letters of attestation that Elite makes available for the Services containing Customer Materials, if any. As used herein, "Security Assessments" means an independent third-party security assessment such as an ISO 27001 certification.

### 3. NOTIFICATION OF SECURITY BREACH

- 3.1 Elite will, without undue delay and within a reasonable period of time, notify Customer of any Security Breach that affects Customer Materials. In the event of any such Security Breach, Elite shall perform a root cause analysis to identify the cause of such Security Breach and shall, upon request, provide to Customer a report detailing the cause of such Security Breach.

Notification(s) of Security Breaches will be delivered to one or more of Customer's contacts by any means Elite selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information. Elite's obligation to report or respond to a Security Breach under this section is not an acknowledgement by Elite of any fault or liability with respect to the Security Breach.

### 4. DEFINITIONS

**Customer Materials** – means information provided to Elite by Customer, which Elite is required to host, use or modify in the provision of a Service.

**Security Breach** – means any actual breach or an unauthorized use or disclosure that directly and adversely impacts the security and confidentiality of Customer Materials.