TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

(Last Updated: May 15, 2023)

1. **Security.** Arcadia shall, during the term of the Agreement, comply in all material respects with the following technical and organizational security measures applicable to the Services:

    a. **General.**

        i. All Arcadia applications that are accessible from the Internet or process personal data are approved prior to launch or implementation by Arcadia's information security.

    b. **Physical Security.**

        i. The equipment hosting the Arcadia Offerings is located in a physically secure facility, which requires badge access at a minimum.

        ii. Physical access to infrastructure housing the Arcadia Offerings is restricted and access allowed based on a need-to-know basis.

        iii. Electronic media (online or offline) and confidential hard copy material is appropriately protected from theft or loss.

    c. **Authentication.**

        i. All access to Arcadia systems is controlled by an authentication method involving a minimum of a unique user ID/complex password combination

        ii. Privileged users and administrators use strong authentication.

        iii. Passwords are never stored in clear text.

        iv. Passwords are complex and not easy to guess or crack. Effectiveness of authentication is tested on a regular basis to verify that unauthorized authentication is not easily permitted.

        v. Remote network access is secured by two-factor authentication.

        vi. All activity performed under a User ID is the responsibility of the individual assigned to that user ID. Users do not share their User ID/password with others or allow other employees to use their User ID/password to perform actions.

        vii. Use of generic user accounts is not permitted.

    d. **Authorization.**

        i. Logical or network access to infrastructure housing the Services is restricted and access allowed based on a need-to-know basis.

        ii. Access requests are documented and approved based on a business need utilizing the principle of least privilege.

        iii. Access rights are reviewed on a periodic basis.

iv. Upon termination or resignation of personnel, access is revoked in a timely manner.

e. **Change Management.** Change requests are documented via ticketing system. The change request should contain, at a minimum, the following information.

i. Business justification for the change

ii. Nature of defect (if applicable)/enhancement

iii. Testing required

iv. Back-out procedures

v. Systems affected

vi. User contact

vii. The process to review and approve change requests must be documented. The process must include management approval.

f. **Network Security.**

i. Industry standard firewalls are implemented to protect the application environment and associated data from the Internet and untrusted networks.

ii. Inbound and outbound connections are denied unless expressly allowed.

iii. Firewall events are monitored in order to detect potential security events.

iv. Network Intrusion Detection or Prevention Systems (NIDS/NIPS) are implemented to monitor traffic for applications handling confidential information.

v. Effectiveness of controls are tested on a periodic basis.

g. **Logging and Monitoring.** Security relevant events, including, but not limited to, login failures, use of privileged accounts, changes to access models or file permissions, modification to installed software, or the operating system, changes to user permissions, or privileges or use of any privileged system function, are logged on all systems.

h. **System Security.**

i. Systems are securely configured according to a security baseline. This baseline includes removing unnecessary services and changing default, vendor-supplied or otherwise weak user accounts and passwords.

ii. System components maintain current security patch levels.

iii. Web servers are hardened according to a secure baseline.

iv. Web servers are configured to accept requests for only authorized and published directories. Default sites, executable or directory listings are disabled.

v. An inventory of technology used to store or process Client data is maintained.

i. **Security Awareness.** Arcadia will design and maintain a Security Awareness program that will train employees upon hire and annually afterwards maintain regular touchpoints with employees on emerging threats.

j. **Device and Media Control.**

i. Arcadia will maintain a device management platform ensuring endpoint controls (e.g.

antivirus/antimalware, disk encryption, patching) are applied uniformly to user endpoints.

ii. Arcadia will encrypt Client data utilizing at minimum TLS 1.2 in transit and AES-256 at rest.

iii. Arcadia will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with Industry Best Practices for media sanitization.

2. **Viruses and Disabling Code**. Arcadia will use commercially reasonable efforts to avoid introducing any viruses, time or logic bombs, Trojan horses, worms, timers, clocks, trap doors, or other computer instructions, devices, or techniques that erase data or programming, infect, disrupt, damage, disable, or shut down the Services, including, without limitation, its security or data. In the event a virus or similar item is found to have been introduced into Arcadia's system, Arcadia will: (a) use commercially reasonable efforts to reduce or eliminate the effects of the virus or similar item; and (b) if the virus or similar item causes a loss of operational efficiency or loss of data, mitigate and restore.

3. **Incident Reporting/Investigation.** Arcadia shall notify Client of any confirmed security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client data ("Data Breach") without undue delay , unless otherwise prohibited by state or federal law. Arcadia will provide Client with regular updates with any new details regarding the Data Breach. A report about the Data Breach will be provided to Client as soon as reasonably practicable and after considering appropriate precautions or limitations such as attorney-client privilege.

4. **Investigations.** Upon written notice to Arcadia, Arcadia shall assist and support Client in the event of an investigation by any regulator, including a data protection regulator, or similar authority, if and to the extent that such investigation relates to personal data handled by Arcadia on behalf of Client. Such assistance shall be at Client's sole expense, except where such investigation was required due to Arcadia's gross negligence.

5. **Audit**. Arcadia will periodically review control effectiveness and remediate any deficiencies identified.