The Training Arcade®

Security Program Overview

The Game Agency maintains a security program intended to safeguard the confidential information of subscribers to The Training Arcade® and the personal data of their authorized users. The purpose of this document is to provide an overview of the security program as of March 1, 2023. As with any effective security program, the policies, controls, and procedures are regularly reviewed and updated as required to meet risk management objectives and evolving industry standards. The information in this document is confidential to The Game Agency, and subject to updates.

The Training Arcade® is a hosted, multi-tenant solution. Maintaining an appropriate level of security for all subscribers requires the consistent application of security controls. It may therefore not be possible to accommodate non-standard access requests or unique security requirements in this shared environment. If a multi-tenant environment does not meet your business or legal requirements, please contact the account executive with whom you are working to discuss potential alternative solutions to your gamification and game-based learning needs.

When assessing security controls, it is important to recognize that, by default, the only personally identifiable information ("**PII**" or "**Personal Data**") stored within the system is the Personal Data of the subscriber's administrators and the data fields specifically designated by the subscriber's administrator associated with the learners playing the training games or accessing the Arcades™ gamification. While some of our subscribers will deploy the training games in an anonymous manner, typically the Personal Data corresponding to an authorized user designated for collection, processing, and storing within our platform are as follows: (i) first name, (ii) last name, (iii) email address, (iv) unique identifier such as employee ID # (if the email address is not used as the unique identifier), (v) internet protocol address ("IP Address") and (vi) the data associated with the game ranking/leaderboard and game analytics. The Personal Data is used to to gate access to the service, provide the permitted level of service to each authorized user, and associate the relevant service activity for each authorized user. Our use of the Personal Data is governed by our privacy policy found at this link: https://thetrainingarcade.com/privacy-policy/

In accordance with generally accepted privacy principles, we recommend that our subscribers request only the minimum required personal data from their authorized users. Additional information, such as the learner's department, region, or team name is only collected if the subscriber's administrator specifically configures the service to do so. Please note that we strictly forbid collecting some types of information from authorized users. Such prohibited data, sometimes called sensitive personal data, includes, but is not limited to, government issued identification numbers, credit card information, and health information. For a complete list, please see the definition of prohibited data by visiting the Content Guidelines and Restrictions section of our website located at this link: https://thetrainingarcade.com/guidelines-and-restrictions/.

As part of delivering our multi-tenant solution, The Game Agency does not access clients' facilities, hardware,or information systems. Since our service is hosted on Amazon Web Services ("**AWS**"), on-site inspections of our premises are also not applicable.

Security Governance

The security program is formally documented, including written policies and a control framework. Employees and contractors who work on The Training Arcade® and have access to confidential information or Personal Data used by the service are required to review and comply with all applicable policies. Roles and responsibilities are clearly defined and communicated.

We are in the process of aligning our security program with the ISO/IEC 27001:2022 standard with the goal of achieving Information Security Management System (ISMS) certification in 2023. In addition, the security program is designed to comply with local and international legislation, including GDPR and CCPA.

We currently use the OneTrust Security Assurance Platform to centralize policies and controls, collect evidence, and support both internal and external audits. Access to more in depth security documentation is available upon request and the execution of a non-disclosure agreement.

Risk Assessments

The Game Agency conducts and reviews risk assessments at least annually. In addition, an appropriate risk review is conducted:

- When significant purchases, acquisitions or procurements are made
- As part of the system development process
- When changes are to be made to the infrastructure
- Upon significant changes in vendor and business partner relationships, and
- When changes in regulatory, economic, or physical environments occur.

Risk assessments and reviews are undertaken to ensure that appropriate security controls are in place to mitigate risks to an acceptable level.

Physical Security

The Training Arcade® is hosted on AWS which is ISO/IEC 27001 certified, and we have reviewed their SOC 2 Type 2 report. Neither The Game Agency nor our subscribers have physical access to cloud provider data centers. The cloud providers are solely responsible for the physical security of their environments.

Personnel Security

The Game Agency conducts background screening commensurate with the individual's responsibilities, and in accordance with applicable laws and regulations.

Security Awareness

The Game Agency maintains a security awareness training program. Employees are required to participate in training at least annually on topics such as:

- Policy, legal, regulatory, and contractual compliance
- Phishing, malware, and ransomware
- Protecting customer data
- Theft of intellectual property
- Theft of cloud computing resources
- Fraud
- Incident management
- Business continuity and disaster recovery

New Employees are expected to review security awareness training and complete a security awareness quiz, delivered of course using The Training Arcade.

Information Classification and Handling

Information is classified and handled according to its classification as required by policy, legal, regulatory, and contractual obligations. Company and customer information is only used for the intended purpose and in accordance with contractual commitments.

Production data is not used in non-production environments.

Access Control

The Game Agency manages access control on a least privilege basis. Requests must be submitted and approved before access is granted. Initial credentials, including passwords, are communicated securely to authenticated individuals. The use of shared accounts is prohibited unless an exception has been formally granted in support of a legitimate business requirement.

Where technically feasible, role-based access controls are used to simplify account management and promote consistent access to resources.

Accounts are disabled or removed promptly when an individual leaves the organization or no longer requires access due to a role change. In addition, account access reviews are conducted at least quarterly.

Our internal password policies are consistent with leading industry practices and automatically enforced where technically feasible. This includes a minimum password length and requirements to change all default passwords.

Where our products allow customers to configure their own password policies through SSO integration, it is the customer's responsibility to ensure that the password configuration meets their security requirements.

Cloud Account Security

Access to our cloud accounts for company infrastructure is restricted and monitored. Multi-factor authentication is required.

Network Security

While AWS maintains the secure foundation upon which The Training Arcade® operates, in accordance with the shared responsibility models, The Game Agency is responsible for some aspects of network security. Our approach to network security includes:

- Data is protected during transit using modern, industry-standard protocols such as TLS.
- Only required services, such as HTTPS, are exposed to the internet.
- Maintenance access is restricted to authorized personnel. System administrators must first connect to the environment using VPN or SD-WAN before they are able to connect and authenticate to individual computing resources.
- SSH access to Linux virtual machines requires cryptographic authentication.
- Network-level access controls are configured to deny access to all resources except as required for the system to function.
- Where appropriate, load balancers and firewalls are used to further reduce the attack surface.
- All established network sessions are terminated after a period of inactivity.
- Logging is enabled and where technically feasible logs are forwarded to a centralized log management platform.
- Cloud provider intrusion detection capabilities are enabled.
- Alerts from the centralized log management platform and intrusion detection systems are sent to the appropriate IT team for investigation.

Server Security

Servers are hardened, kept up-to-date, and comply with all applicable security policies, including access control, cryptography, and vulnerability management.

Workstation Security

Workstations are kept up-to-date, require users to authenticate, use full disk encryption, and have endpoint protection software installed.

Software and System Design

The Game Agency designs and implements systems taking into account confidentiality, integrity, and availability requirements.

Cryptography

The Game Agency uses modern, commercially accepted cryptography with key sizes that meet or exceed commercial best practices. All data transmitted over public networks is encrypted. All

data stored by The Game Agency is encrypted at rest. Keys for applications such disk volume and database encryption are managed by AWS.

Vendor Management (Third Parties & Subcontractors)

For those vendors who will have access to a subscriber's confidential information or Personal Data, the Game Agency conducts a risk review, reviews the vendor's security certifications and compliance reports (such as ISO/IEC 72001, SOC 2, PCI DSS, etc.), and where required, issues a risk assessment questionnaire to the vendor.

Contracts with such vendors clearly define roles and responsibilities of the vendor and applicable security requirements. These vendors are required to immediately notify The Game Agency in the event of a security incident that involves The Training Arcade® data. Upon termination of services, access to any of our systems by such vendors is immediately disabled, and they are required to return or destroy all data belonging to The Game Agency or a subscriber.

Backups

Appropriate backup procedures are in place to safeguard information and facilitate disaster recovery procedures. We currently back up The Training Arcade® daily.

Change Management

The Game Agency follows documented change management policies and procedures.

Business Continuity, Disaster Recovery, and Incident Management

The Training Arcade® architecture includes load balancers, redundant servers, and the ability to scale the system as required.

The Game Agency maintains business continuity, disaster recovery, and incident response plans, supported by appropriate policies and training. Plans are tested at regular intervals to ensure that they remain accurate and relevant.

In the event of a security incident involving customer data, The Game Agency will notify the subscriber's administrators within two (2) business days of becoming aware of the incident.

Vulnerability Management

The Game Agency has an established vulnerability management program including policies and procedures for discovering, evaluating risk and treating vulnerabilities. Tenable.io is used to scan systems on a regular basis and report findings to security and IT operations personnel.

Vulnerabilities are triaged and updates are applied in a reasonable time, taking into account the severity of the vulnerability and the resulting risk.

A third-party is retained to conduct penetration tests on all production systems at least once per year, and when significant changes occur that could impact the security of the system.

Contact Information

If you have any specific questions about our security program, please do not hesitate to reach out to support@thetrainingarcade.com, and we'll get back with you as soon as possible. Thank you!