SECURITY MEASURES

Version 1.0
December 2020

support@immersivelabs.co.uk | www.immersivelabs.com | +44 (0)20 3893 9101 | @immersivelabs

What do we think about information security?

We enable our customers to improve the skills of their staff through gamified training. Naturally, we also maintain a strong security posture ourselves. Threats and technology continually change, and our security team ensures we evolve to face these threats, giving our clients the confidence that we are protecting their data optimally. We exercise the same care handling data as we do upskilling cybersecurity workforces, and our dedicated information security team work alongside our cybersecurity experts who develop our labs.

On this page we have condensed our security controls and measures into a short but sweet summary. We also provide information about the way we process personal data which you can access via the Privacy and Data Protection section accessible via **www.immersivelabs.com/legal**. Feel free to contact us at **legal@immersivelabs.com** if you would like more information regarding our security posture and how we handle customer and personal data.

Organizational security

Our employees complete our security awareness learning path when they join the company. We also conduct regular learning sessions, wherein our security experts deep dive into a particular security subject to expand company-wide knowledge.

Executives are also embedded in the security culture. Security is a top priority, and the information security team conducts weekly catch-ups with every executive, discussing issues, potential threats and how to improve best practices. Our monthly Security and Risk Review (SaRR) focuses on strategy, governance and risk management.

Antivirus software (Sophos) is enabled and updated on every workstation, daily backups are performed on workstations to speed up recovery. End-users are as important as the technology we use, so we take great pride in securing our employees and empowering them with the tools and training they need to perform securely.

Architectural security

Data encryption

Every workstation's hard drive is encrypted, and decryption keys are securely stored. AWS encrypts all data stored in the platform using an industry standard AES-256 encryption algorithm. All data in transit is encrypted using Transport Layer Security (TLS) 1.2, again using an industry standard AES-256 cipher.

Access control

Immersive Labs' employees use multi-factor authentication. Every application used to operate Immersive Labs is assigned a business owner who regularly reviews access rights and privileges.

We follow the "least-privilege" and "mandatory vacation" principles. They enable us to limit attack surface in case of an account compromise and ensure access to critical applications is tightly controlled.

Access to infrastructure and key applications is monitored, logged and aggregated, and a team investigates alerts in case of abnormal activities.

Operational security

Physical security

Immersive Labs applications are hosted in AWS state-of-the-art data centres designed to protect mission-critical computer systems with fully redundant subsystems and hierarchized security zones. AWS data centres adhere to the strictest physical security measures, including the following:

- Multiple layers of authentication for accessing server areas
- Multi-factor biometric authentication for critical areas
- Camera surveillance systems at internal and external entry points
- 24/7 monitoring by security personnel

All physical access to the data centres is highly restricted and stringently regulated.

Network security

Immersive Labs has established detailed operating policies, procedures and processes designed to help manage the overall quality and integrity of the Immersive Labs environment. As the company is cloud-native, we enforce network segregation through different VPCs for staging and production environments and implement security groups. Being cloud-native means enforcing proper access control is at the forefront of network security; we follow a zero-trust architecture model.

Engineers have to access their environments using a dedicated virtual private network (VPN) to prevent data leakage, and engineering managers conduct periodic access reviews.

Application security

Immersive Labs has implemented an enterprise secure Software Development Life Cycle (SDLC) to help ensure the continued security of our training platform.

Our engineers follow custom application security training to enhance the development process and champion secure coding practices. We conduct quarterly penetration tests on our systems with internal security experts. Processes manage the remediation of vulnerabilities with weekly triage meetings and complete involvement of engineering.

Continuity of operations

Our platform is constantly evolving, but availability is at the top of our objectives. The disaster recovery plan for the infrastructure is regularly tested, and the platform can be rapidly rebuilt in case of an availability loss. This is possible thanks to the frequent backups to facilitate rollbacks.

Processes for business continuity, incident response and crisis management define roles, responsibilities, procedures, and playbooks to ensure our platform is available continuously.

Compliance

We currently hold Cyber Essentials certification. We are undergoing an ISO 27001 audit and working on Cyber Essentials Plus.