DIGITAL ONBOARDING

Security & Compliance

October 2021

Compliance

Digital Onboarding reviews applicable regulations in jurisdictions where it does business and updates company policies accordingly.

Digital Onboarding is SOC 2 Type 2 compliant.

IT Governance

The control environment at Digital Onboarding begins at the highest level of the Company. Executive leadership plays an important role in establishing the Company's core values and principles. Security responsibilities are assigned to Digital Onboarding team members to monitor the effectiveness of and adherence to the security controls, but also in the maintenance of the security policies and procedures. There is active management involvement in the review of the security program that assures that the organization takes security seriously.

Security Policies and Standards

Digital Onboarding's Information Security policies and standards are reviewed and evaluated annually and also if changes occur within Digital Onboarding that affects a particular approved policy or standard. The policies are distributed and communicated to all employees with supportive guidance and compliance requirements.

Infrastructure Security

Digital Onboarding has designed and implemented a large-scale, mission-critical SaaS solution that only requires that participants have access to the internet and a modern web browser. Digital Onboarding provides its services using multiple servers and supporting network components in world-class data centers.

Cyber Insurance

Digital Onboarding has cyber insurance to protect the businesses from Internet-based risks, and more generally, from risks relating to information technology infrastructure, information privacy, information governance liability, and activities.

Risk Assessment

Digital Onboarding Risk Management Program is a function that is responsible for identifying potential business risks from multiple IT sources, such as the company's use of technology while serving clients, coordinating client security inquiries in support of their due diligence requests, performing risk assessments to evaluate potential IT risks, and providing input concerning risk management plans which help to minimize and maintain IT risks to an acceptable level.

Security Awareness Training

The privacy and security awareness and training program is available to employees and contractors of Digital Onboarding and is mandatory upon employment or engagement and then on a periodic basis.

Security Incident Management

Digital Onboarding implements policies and procedures to address the handling of security incidents. A security incident is an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Application Security

The Digital Onboarding platform forces secure sessions and provides customer-specific login policies. The platform is built on application security development best practice (OWASP) that prevents the following vulnerabilities: weak server-side controls, insecure data storage, insufficient transport layer protection, unintended data leakage, broken cryptography, client- side injection, security decisions via untrusted inputs, improper session handling, and lack of binary protections.

Encryption

Digital Onboarding utilizes technologies or methodologies that make client data unusable, unreadable, or indecipherable to unauthorized individuals, including mechanisms to encrypt client data at rest and in motion whenever possible.

Access Control

Management enforces policies and procedures to ensure that only those that require access to client data have the appropriate level of access consistent with their job responsibility. Access management procedures are enforced through roles and an approval process based on the segregation of duties.

Business Continuity and Disaster Recovery

Recognizing the need for responding to an emergency or a natural/made threat that damages systems that contain client data or to assist federal or local authorities, Digital Onboarding maintains plans for data backup, business continuity, and disaster recovery.

Vendor Management

Digital Onboarding vendor choices have implications for their clients. Products are chosen as best of breed with the capability to truly differentiate themselves in the marketplace. To support this, Digital Onboarding established a vendor management program. The purpose of the vendor management program is to incorporate assessments of performance, functionality, value and risk when selecting vendors with whom they do business.

Vulnerability Management

Digital Onboarding has implemented a vulnerability management process that is focused on mitigating and remediating the risks associated with the software and hardware used in their infrastructure. Digital Onboarding takes these risks seriously as they could have a significant negative impact on business assets.

Change Management

The change management process has been established to provide a layer of protection for the Company by ensuring that every change performed is thoroughly discussed and is approved prior to migration to production.

Logging and Monitoring

Digital Onboarding has established a Logging and Monitoring Program. Practices outlined within this program address identifying system/network issues, escalating issues to support teams and effective communications regarding problem determination and resolution.

Endpoint Protection

MacOS and Windows endpoints are configured with anti-malware protections. Windows endpoints are configured to check for malware and virus definitions daily. Full disk encryption is configured and enforced on all end user laptops and desktops. Decryption keys are transferred and escrowed securely. End-user systems are configured to prevent end-user decryption of disks with reporting and remediation processes in place for exception management if necessary.

Monitoring

Threats to the security of systems and the information they contain are evolving at a faster pace. Digital Onboarding understands that it must periodically review not only its policies and procedures to respond to these changes but adjust its corresponding security controls to be consistent with the policies and procedures by publishing and enforcing additional guidelines.