An Overview of Information Security at OneSpan
Version: September 2023

Optimizing security efforts and resources to properly protect OneSpan information systems and information assets requires a structured approach to identify the various assets needing to be protected, their relative importance to OneSpan, and the risks faced by such assets. At least annually, we identify the security measures already in place, assess their effectiveness to help measure the residual risk, and prioritize any changes that would be required to lower the risk to an acceptable level for OneSpan.

Governance
OneSpan's Information Security Risk Management Policy formalizes everyone's responsibility, from senior managers to individual users, in minimizing information security risks. The policy is approved by the Information Security Steering Committee, is reviewed on a yearly basis to account for changes in OneSpan's risk environment, and describes a formal process to identify, assess and track key information security risks. When required, a risk treatment plan is implemented to bring risk levels below acceptable risk tolerance.

OneSpan's Information Security Steering Committee is composed of key senior leaders who operate under a formal charter. Their role is to oversee the corporate information security program and OneSpan's security posture. Their role also includes tracking progress on information security risks and approving and tracking risk-reduction initiatives. The Information Security Steering Committee conducts regular meetings, at least quarterly, with OneSpan's Chief Information Security Officer.

OneSpan's Board of Directors also oversees the progress of the information security program and the variation of information security risks through quarterly information security briefings, at a minimum. The Audit Committee, which consists solely of independent directors, has the primary responsibility for this oversight.

Insurance
OneSpan maintains customary cybersecurity risk insurance that includes access to a data breach management assistance unit if required and utilizes the services of an independent insurance broker that also provides insurance advisory support.

Reviews and Certifications
For internal OneSpan information systems and information assets, we conduct regular internal reviews and employ continuous security monitoring. To provide additional assurance, OneSpan conducts periodic independent reviews of the key components of its security program. These reviews are carried out by individuals independent of the area under review. Areas for review and the schedule for such reviews are determined based on their criticality.

For customer facing products and services, in addition to internal reviews and testing, we undergo various external reviews and certifications. Some of our products are certified under specific technical standards or industry guidelines, such as European banking regulations referred to as PSD2. In addition, our cloud platforms for SaaS solutions are audited annually by external independent auditors. The auditors review our platforms against the Service Organization Controls (SOC) 2 and ISO 27001, 27017 and 27018 standards. We receive annual certifications under these audits.

In addition, we conduct self-certification activities for those standards or regulations that are not covered by the external auditors, such as the General Data Protection Regulation (GDPR) in the European Union and European Economic Area and Health Insurance Portability and Accountability Act (HIPAA) regulations in the United States.

Technical and organizational measures

OneSpan's list of technical and organizational measures are to be found here (link).

Engagement of independent external data protection officer (DPO)

To help ensure compliance with applicable data protection law and to assist in addressing data breaches involving personal data, Supplier has engaged an independent external data protection officer with a third party DPO certification and GDPR lead auditor certification. The DPO has also taken chief information security officer certification courses. The DPO undergoes yearly update training and monitors changes in data protection law, supported by a data protection information system which includes global data guidance and data protection management (OneTrust).

Third-party risks

OneSpan's vendor security risk management program covers all vendors that require connectivity to OneSpan systems or access to OneSpan confidential information. Security reviews are performed periodically, based on vendor criticality, to identify potential security issues with the vendor systems or practices.

Training

In order to reduce the likelihood and impact of security incidents, OneSpan has implemented a global security awareness training program that includes mandatory security and data protection awareness training for all personnel at hire time and yearly thereafter. Additional training is made available to personnel as required based on their role. This includes secure development training for developers, in support of OneSpan's secure development lifecycle, as well as incident response training.

In response to the various phishing attacks that often are at the root of security breaches, and in addition to the various technical controls that are in place, OneSpan has implemented recurring phishing campaigns that target its employees in order to improve their ability to recognize and report phishing messages. Employees who respond inappropriately to internal phishing campaigns receive additional remedial training.