Security Overview

This oneapp Security Overview (“Security Overview”) is incorporated into and made a part of the Terms of Service between oneapp and Merchant covering Merchant’s use of the SaaS (as defined below) (“Agreement”).

1. Definitions

“SaaS” means any services or application programming interfaces branded as “oneapp”.

Any capitalized term not defined in this Section 1 will have the meaning provided in the Agreement, this Security Overview, or the Data Protection Addendum. The then-current terms of the Data Protection Addendum are available at https://legal.withoneapp.com/#data-protection-addendum.

2. Purpose. oneapp maintains data security policies and procedures in accordance with Applicable Data Protection Law, which includes the New York "Stop Hacks and Improve Electronic Data Security Act (“SHIELD Act”). This Security Overview describes oneapp’s security program, security certifications, and technical and organizational security controls to protect (a) Merchant Data from unauthorized use, access, disclosure, or theft and (b) the SaaS. As security threats change, oneapp continues to update its security program and strategy to help protect Merchant Data and the SaaS. As such, oneapp reserves the right to update this Security Overview from time to time; provided, however, any update will not materially reduce the overall protections set forth in this Security Overview. The then-current terms of this Security Overview are available at https://legal.withoneapp.com/#security-overview. This Security Overview does not apply to any (a) SaaS that are identified as alpha, beta, not generally available, limited release, developer preview, or any similar SaaS offered by oneapp or (b) services provided by third party vendors.

3. Security Organization and Program. oneapp maintains a risk-based assessment security program. The framework for oneapp’s security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the SaaS and confidentiality, integrity, and availability of Merchant Data. oneapp’s security program is intended to be appropriate to the nature of the SaaS and the size and complexity of oneapp’s business operations. oneapp has separate and dedicated Information Security teams that manage oneapp’s security program. There is a team that facilitates and supports independent audits and assessments performed by third parties. oneapp’s security framework is based on the ISO 27001 Information Security Management System and includes programs covering: Policies and Procedures, Asset Management, Access Management, Cryptography, Physical Security, Operations Security, Communications Security, Business Continuity Disaster Recovery Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, and Security Monitoring and Incident Response. Security is managed at the highest levels of the company, with oneapp’s Chief Information Officer (“CIO”) meeting with executive management regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are reviewed and approved by management at least annually and are made available to all oneapp employees for their reference.

4. Confidentiality. oneapp has controls in place to maintain the confidentiality of Merchant Data in accordance with the Agreement. All oneapp employees and contract personnel are bound by oneapp’s internal policies regarding maintaining the confidentiality of Merchant Data and are contractually obligated to comply with these obligations.

5. People Security

5.1 Employee Background Checks. oneapp performs background checks on all new employees at the time of hire in accordance with applicable local laws. oneapp currently verifies a new employee’s education and previous employment and performs reference checks. Where permitted by applicable law, oneapp may also conduct criminal, credit, immigration, and security checks depending on the nature and scope of a new employee’s role.

5.2 Employee Training. At least once (1) per year, oneapp employees must complete a security and privacy training which covers oneapp's security policies, security best practices, and privacy principles. Employees on a leave of absence may have additional time to complete this annual training. oneapp's dedicated security team also performs phishing awareness campaigns and communicates emerging threats to employees. oneapp has also established an anonymous hotline for employees to report any unethical behavior where anonymous reporting is legally permitted.

6. Third Party Vendor Management

6.1 Vendor Assessment. oneapp may use third party vendors to provide the SaaS. oneapp carries out a security risk-based assessment of prospective vendors before working with them to validate they meet oneapp's security requirements. oneapp periodically reviews each vendor in light of oneapp's security and business continuity standards, including the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal or regulatory requirements. oneapp ensures that Merchant Data is returned and/or deleted at the end of a vendor relationship. For the avoidance of doubt, telecommunication providers are not considered subcontractors or third-party vendors of oneapp.

6.2 Vendor Agreements. oneapp enters into written agreements with all of its vendors which include confidentiality, privacy, and security obligations that provide an appropriate level of protection for Merchant Data that these vendors may process.

7. Security Certifications and Attestations. oneapp holds the following security-related certifications and attestations from third party vendors: ISO/IEC 17001, ISO/IEC/ 170017 & 27018, SOC 2 Type 2, PCI DSS Level 1, and PCI DSS Level 4.

8. Hosting Architecture and Data Segregation

8.1 Amazon Web Services.The SaaS are hosted on Amazon Web Services ("AWS") in the United States of America and protected by the security and environmental controls of Amazon. The production environment within AWS where the SaaS and Merchant Data are hosted are logically isolated in a Virtual Private Cloud (VPC). Merchant Data stored within AWS is encrypted at all times. AWS does not have access to unencrypted Merchant Data. More information about AWS security is available at https://aws.amazon.com/security/ and https://aws.amazon.com/compliance/shared-responsibility-model/. For AWS SOC Reports, please see https://aws.amazon.com/compliance/soc-faqs/.

8.2 Google Cloud Platform. oneapp uses Google Workspace for internal and external office productivity and communications, hosted on Google Cloud Platform ("GCP") in the United States of America. More information about GCP security is available at https://cloud.google.com/architecture#security.

8.3 SaaS. For the SaaS, all network access between production hosts is restricted, using access control lists to allow only authorized services to interact in the production network. Access control lists are in use to manage network segregation between different security zones in the production and corporate environments. Access control lists are reviewed regularly. oneapp separates Merchant Data using logical identifiers. Merchant Data is tagged with a unique customer identifier that is assigned to segregate Merchant Data ownership. The oneapp APIs are designed and built to identify and allow authorized access only to and from Merchant Data identified with customer specific tags. These controls prevent other customers from having access to Merchant Data.

9. Physical Security. AWS data centers are strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication (2FA) a minimum of two (2) times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions. Each data center has redundant electrical power systems that are available twenty-four (24) hours a day, seven (7) days a week. Uninterruptible power supplies and on-site generators are available to provide back-up power in the event of an electrical failure. In addition, oneapp headquarters and office spaces have a physical security program that manages visitors, building entrances, closed circuit televisions, and overall office security. All employees, contractors, and visitors are required to wear identification badges.

10. Security by Design. oneapp follows security by design principles when it designs the SaaS. oneapp also applies the oneapp Secure Software Development Lifecycle (Secure SDLC) standard to perform numerous security-related activities for the SaaS across different phases of the product creation lifecycle from requirements gathering and product design all the way through product deployment.

These activities include, but are not limited to, the performance of (a) internal security reviews before deploying new SaaS or code; (b) penetration tests of new SaaS by independent third parties; and (c) threat models for new SaaS to detect potential security threats and vulnerabilities.

11. Access Controls

11.1 Provisioning Access. To minimize the risk of data exposure, oneapp follows the principles of least privilege through a team-based-access-control model when provisioning system access. oneapp personnel are authorized to access Merchant Data based on their job function, role, and responsibilities, and such access requires Merchant approval. Access rights to production environments that are not time-based are reviewed at least semi-annually. An employee's access to Merchant Data is promptly removed upon termination of their employment. In order to access the production environment, an authorized user must have a unique username and password and multi-factor authentication enabled. Before an engineer is granted access to the production environment, access must be approved by management and the engineer is required to complete internal training for such access including training on the relevant team's systems. oneapp logs high risk actions and changes in the production environment. oneapp leverages automation to identify any deviation from internal technical standards that could indicate anomalous/unauthorized activity to raise an alert within minutes of a configuration change.

11.2 Password Controls. oneapp's current policy for employee password management follows the NIST 800-63B guidance, and as such, our policy is to use longer passwords, with multi-factor authentication, but not require special characters or frequent changes. When a customer logs into its account, oneapp hashes the credentials of the user before it is stored.

12. Change Management. oneapp has a formal change management process it follows to administer changes to the production environment for the SaaS, including any changes to its underlying software, applications, and systems. Each change is carefully reviewed and evaluated in a test environment before being deployed into the production environment for the SaaS. All changes, including the evaluation of the changes in a test environment, are documented using a formal, auditable system of record. A rigorous assessment is carried out for all high-risk changes to evaluate their impact on the overall security of the SaaS. Deployment approval for high-risk changes is required from the correct organizational stakeholders. Plans and procedures are also implemented in the event a deployed change needs to be rolled back to preserve the security of the SaaS.

13. Encryption. For the SaaS, (a) the databases that store Merchant Data are encrypted using the Advanced Encryption Standard and (b) Merchant Data is encrypted when in transit between Merchant's software application and the SaaS using TLS v1.2.

14. Vulnerability Management. oneapp maintains controls and policies to mitigate the risk of security vulnerabilities in a measurable time frame that balances risk and the business/operational requirements. oneapp uses a third-party tool to conduct vulnerability scans regularly to assess vulnerabilities in oneapp's cloud infrastructure and corporate systems. Critical software patches are evaluated, tested, and applied proactively. Operating system patches are applied through the regeneration of a base virtual-machine image and deployed to all nodes in the oneapp cluster over a predefined schedule. For high-risk patches, oneapp will deploy directly to existing nodes through internally developed orchestration tools.

15. Penetration Testing. oneapp performs penetration tests and engages independent third-party entities to conduct application-level penetration tests. Security threats and vulnerabilities that are detected are prioritized, triaged, and remediated promptly. oneapp maintains a Bug Bounty Program through Bug Crowd, which allows independent security researchers to report security threats and vulnerabilities on an ongoing basis.

16. Security Incident Management. oneapp maintains security incident management policies and procedures in accordance with NIST SP 800-61. oneapp's Security Incident Response Team ("T-SIRT") assesses all relevant security threats and vulnerabilities and establishes appropriate remediation and mitigation actions. oneapp retains security logs for one hundred and eighty (180) days. Access to these security logs is limited to T-SIRT. oneapp utilizes third-party tools to detect, mitigate, and prevent Distributed Denial of Service (DDoS) attacks.

17. Discovery, Investigation, and Notification of a Security Incident. oneapp will promptly investigate a Security Incident upon discovery. To the extent permitted by applicable law, oneapp will notify Merchant of a Security Incident in accordance with the Data Protection Addendum. Security Incident notifications will be provided to Merchant via email to the email address designated by Merchant in its account.

18. Resilience and Service Continuity

18.1 Resilience. The hosting infrastructure for the SaaS (a) spans multiple fault-independent availability zones in geographic regions physically separated from one another and (b) is able to detect and route around issues experienced by hosts or even whole data centers in real time and employ orchestration tooling that has the ability to regenerate hosts, building them from the latest backup.

18.2 Service Continuity. oneapp also leverages specialized tools available within the hosting infrastructure for the SaaS to monitor server performance, data, and traffic load capacity within each availability zone and colocation data center. If suboptimal server performance or overloaded capacity is detected on a server within an availability zone or colocation data center, these specialized tools increase the capacity or shift traffic to relieve any suboptimal server performance or capacity overload. oneapp is also immediately notified in the event of any suboptimal server performance or overloaded capacity.

19. Merchant Data Backups. oneapp performs regular backups of Merchant Data, which is hosted on AWS's data center infrastructure. Merchant Data that is backed up is retained redundantly across multiple availability zones and encrypted in transit and at rest using the Advanced Encryption Standard.