Security Controls Overview

Processes

Change Management

Any changes to our production environments are reviewed and approved by the Woop Change Management Team (CMT). Change approvals involve risk assessment, test and rollback plans. Approved deployments are primarily scheduled during off-peak times to minimize disruptions, and exceptional situations such as critical system patches/ updates and hot fixes are deployed as needed, after consideration and approval of the CMT.

Vendor Risk Management

Our vendor risk management processes identify and protect our business data and intellectual property which may be hosted/stored on third-party platforms. Woop requires assessments of all third-party vendors for data security and compliance. Our vendors undergo annual re-evaluation.

Identity & Access

Access to our production systems and services by employees are based on a role-based, need-to-know model with least privileges. We systematically monitor user accounts using behavioral analytics and anomaly detection. Multi-factor authentication is required for access to Woop networks and systems.

Governance, Risk, & Compliance (GRC)

We maintain PCI-DSS compliance, targets SOC2 compliance and attestation, and we support CCPA and NYDFS. All of WOOP's information security policies, processes, programs, standards, and guidelines, are managed and monitored through our centralized GRC platform.

NETWORK SECURITY: Our network environment is monitored 24x7, aggregating Woop's internal security processes, along with traffic monitoring, intrusion prevention and detection of our cloud infrastructure providers, including Microsoft Azure, Microsoft Office 365 and Mongo Atlas.

VULNERABILITY MANAGEMENT: Vulnerability and policy scans are systematically performed on our network environments and applications. A variety of tools, including Microsoft Azure Security Center, scan Woop's assets on a daily basis.

APPLICATION SECURITY: The Woop Platform Development Team adheres to the latest coding standards and security best practices, utilizing Security Information and Event Management (SIEM) tools to track developer behavior and anomalies.

ENDPOINT SECURITY: All systems including servers, desktops, laptops and mobile devices are centrally managed and fully encrypted. WOOP remote systems connect via secure VPN to our secured networks.

THIRD-PARTY PENETRATION TESTING: We engage independent cybersecurity experts to perform external penetration testing against our applications and networks on a frequent, but random basis, while performing quarterly penetration self-testing.

LOG/EVENT MANAGEMENT: Security and application logs are centrally stored and analyzed in real-time by Woop's security information and event management systems. Our security operations center monitors events and alerts 24x7.

INCIDENT MANAGEMENT: Woop's Confidentiality and Security Team (CST) formalizes incident management processes, assembling teams for incident response, investigation, escalation, and resolution – followed by post-mortem retrospectives and enhancement processes

Physical Security

Physical access to our offices are restricted and controlled by programmable key fobs and id badges. Access points are under 24x7 video surveillance. Vendors and guests sign-in to visitor logs, and are provided visitor badges to wear prominently. A staff member escorts visitors at all times. Data Centers(DC) hosting equipment is certified PCI-DSS, SOC2, or ISO 27001:2013 compliant. All physical DC locations provide multiple layered facets of security, including biometrics, physical guards, cameras, and secure equipment racks/cages.

Personnel Security

We perform pre-hire background checks on all prospective employees and independent contractors . Once hired, each staff member completes our security awareness training, and re-certifies on a semi-annual basis.