Okta’s Commitment to Security & Privacy

Okta is committed to achieving and preserving the trust of our customers, by providing a comprehensive security and privacy program that carefully considers data protection matters across our suite of products and services.

This documentation describes the security-related and privacy-related practices that Okta follows for the on-premise Okta Access Gateway software product and software updates or modifications ("Updates") to the foregoing (collectively, the "Software").

- Okta has commissioned a third-party review of the Software’s code base, to verify the identity of third-party (including open source) components that are included in the Software. Okta commissions third-party reviews from time to time, as necessary in its discretion, to perform additional reviews of the Software’s code base, if and to the extent that the Software is updated.

- If Okta elects to make any Updates available to customers, it may use a third-party platform provider, such as Amazon Web Services, to assist in doing so.

- Prior to being distributed or otherwise made available to customers, any Updates will be scanned to identify and remediate the Open Web Application Security Project’s top ten application vulnerabilities, to the extent applicable to the Software. As of the drafting date of this document, those application vulnerabilities include: injection, broken authentication, sensitive data exposure, XML External Entities, broken access control, security misconfigurations, cross-site scripting, insecure deserialization, using components with known vulnerabilities, and insufficient logging and monitoring.

- Okta will perform penetration testing of the Software at least once annually.