SECURITY & PRIVACY DOCUMENTATION FOR IDENTITY SECURITY POSTURE MANAGEMENT

(Last updated May 20, 2024)

1. 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.

2. Covered Services

This documentation describes the security and privacy controls and assurances that Okta has in place with respect to Okta's online services branded as Identity Security Posture Management (formerly known as Spera Security) (the "Service"). For avoidance of doubt, this documentation does not apply to Professional Services, Non-Okta Applications, or Free Trial Services made available by Okta, and as such terms are defined in Okta's Master Subscription Agreement, available online at okta.com/agreements. The controls and assurances described herein are designed to ensure the integrity, confidentiality, and availability of all electronic data submitted by customers or on behalf of a customer to the Service ("Customer Data").

3. Service Architecture, Data Segregation & Data Processing

The Service operates in a multitenant architecture that is designed to segregate Customer Data and restrict access to Customer Data based on business needs. The Okta architecture provides an effective logical separation of Customer Data for different customers via customer-specific "Organization IDs," and allows for role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, such as for testing and production.

Okta has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Okta and its sub-processors.

4. Retrieval of Customer Data

Upon written request by a customer made prior to the effective date of termination or expiration of the customer's agreement, Okta will make available to the customer, at no cost, for thirty (30) days following the end of the agreement's term, for download a file of Customer Data (other than personal confidential information such as, but not limited to, User passwords which may not be included except in hashed format) in industry-standard format (e.g. and without limitation, .json or .csv). After such 30-day period, Okta shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, be entitled to delete all Customer Data by expunging Customer's unique instance of the Service. During the term of the agreement, Customer may extract Customer Data from the Service in accordance with applicable Documentation.

Okta will not be required to remove copies of the Customer Data from its backup media and servers until such time as the backup copies are scheduled to be deleted in the normal course of business; provided further that in all cases Okta will continue to protect the Customer Data in accordance with the customer's agreement.

5. Secure Deletion of Customer Data

Okta maintains policies and procedures regarding the deletion of Customer Data, taking into account available technology, so that Customer Data cannot be practicably read or reconstructed. Customer Data is deleted using secure deletion methods materially in accordance with applicable NIST guidelines.

6. Customer-Configurable Security Controls

Okta's hosted Service includes a variety of configurable security controls that allow Okta customers to tailor the security of the Service for their own use. Okta personnel will not set a defined password for a User. Each customer's Users are provided with a token that they can use to set their own password in accordance with the applicable customer's password policy. Okta strongly encourages all customers, where applicable in their configuration of the Service's security settings, to use the multi-factor authentication features made available by Okta.

7. Information Security Policy ("ISP")

Okta maintains and implements a comprehensive information security management policy that establishes administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of Okta's business; (b) the amount of resources available to Okta; (c) the type of information that Okta will store and process; and (d) the need for security and protection from unauthorized disclosure of such Customer Data. The ISP is reviewed annually, and may be updated if necessary, based on changes in legal and regulatory requirements

related to privacy and data security practices and industry standards applicable to the Service.

8. Security Certifications.

Okta maintains the following certifications, confirmation of which is available upon a customer's written request:

- ISO 27001

9. Security Audit Report.

Okta will provide a customer, upon its written request, with a copy of Okta's then-current SOC2 Type II (or successor standard) Report which will be issued at least annually by an accredited third-party auditor, including information as to whether the audit revealed any material findings regarding the Service, and if so, the nature of each finding discovered.

10. Assigned Security Responsibility.

Okta assigns responsibility for the development, implementation, and maintenance of its security operations, including:

a) Designating a security official with overall responsibility; and

b) Defining roles and responsibilities for individuals with security obligations.

11. Relationship with Sub-processors.

Okta conducts reasonable due diligence and security assessments of sub-processors engaged by Okta to store and/or process Customer Data ("Sub-processors"). Okta's agreements with Sub-processors contain provisions similar to or more stringent than those provided for in this Security & Privacy Documentation.

12. Background Checks.

Okta performs background checks on any employees who are to perform material aspects of the Service or have access to Customer Data. Where permitted under applicable law, background checks are also performed annually for employees with access to highly-sensitive information.

13. Security & Privacy Awareness and Training.

All Okta employees must acknowledge in writing that they will comply with the ISP and protect Customer Data. For all of its employees, Okta mandates annual privacy and security awareness training programs that address their obligations related to the processing of personal data contained within Customer Data, as well as the implementation of and compliance with the ISP. A disciplinary policy and process are maintained and may be invoked if any Okta employee violates the ISP.

14. Identity and Access Management.

Okta has in place access management policies and procedures that are designed:

a) To limit access to its information systems and the facilities in which they are housed to properly-authorized persons;

b) To prevent personnel and others who should not have access from obtaining access; and

c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

Okta institutes the following identity management controls:

a) Provisioning Okta personnel with access to Customer Data based on need-to-know criteria and the least-privilege principle;

b) Requirements that User identifiers (i.e., User IDs) be unique and readily identifiable to the Okta personnel to whom they are assigned, and no shared or group User IDs be used by Okta personnel for access to any Customer Data;

c) Password and other strong authentication controls, including addressing the number of invalid login requests before locking out, uniqueness, reset, termination after a period of inactivity, password reuse limitations, length, and expiration;

d) Periodic reviews to ensure that those Okta personnel who have access to Customer Data still require access.

15. Physical and Environmental Security.

Okta maintains controls that provide reasonable assurance that access to Customer Data, at the production data center and other Okta-managed facilities, is limited to properly-authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. These controls include:

a) Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;

b) Camera surveillance systems at critical internal and external entry points to the data center;

c) Systems that maintain the air temperature and humidity at appropriate levels for the computing equipment; and

d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

16. Data Encryption.

Okta uses strong encryption to protect Customer Data in-transit and at-rest. Customer Data at-rest is stored on environment(s) that are not accessible from the internet. Encrypted solutions and environments are utilized to protect all backups.

17. Business Continuity and Disaster Recovery.

Okta maintains policies and procedures for responding to an emergency or a force majeure event that causes or could cause Okta's infrastructure to experience a total, or unacceptably degraded, loss of service ("**DR/BC Event**"). Such procedures include:

a) Data Backups: A policy and process for performing periodic backups of production file systems and databases to meet the RPO and RTO described below:

   i. Recovery Point Objective ("**RPO**") is no more than 24 hours;

   ii. Recovery Time Objective ("**RTO**") is no more than 72 hours to restoration of the full Service.

b) Business Continuity Plan ("**BCP**"): A formal process to address how a DR/BC Event that disrupts Okta's non-Service functions (i.e., corporate processes) might be managed in order to minimize loss of vital resources. The BCP, a copy of which is made available to a customer upon written request, is tested annually.

c) Disaster Recovery Plan ("**DRP**"): A formal process for the production environment that addresses how a DR/BC Event that disrupts Okta's Service might be managed to minimize loss of operations. The DRP includes requirements for testing on a regular basis, currently four times a year. Confirmation of such testing is available to a customer upon written request.

18. Secure Development Practices.

Okta adheres to the following development controls:

a) Development Policies: Okta follows secure application development policies, procedures, and standards that are aligned to industry-standard practices, such as the OWASP Top 10 and SANS Top 20 / CIS Critical Security Controls;

b) Training: Okta provides employees responsible for secure application design, development, configuration, testing, and deployment the appropriate (based on role) technical training, on an annual basis, by the security team regarding secure application development practices; and

c) Hardening of workstations used to develop the Service in alignment with US Government-approved frameworks.

19. Malware Control.

Okta employs then-current industry-standard measures to test the Service to detect and remediate viruses, Trojan horses, worms, logic bombs, or other harmful code or programs designed to negatively impact the operation or performance of the Service.

20. Data Integrity and Management.

In addition to the data segregation measures described in Section 3 of this document, Okta maintains policies that ensure the following:

a) Back Up/Archival: Okta maintains full backups of the database(s) containing Customer Data as required to maintain the RPO on secure server(s) or on other commercially acceptable secure media; and

b) Data Integrity Checks: Okta implements automated and manual processes to ensure input and output integrity of Customer Data.

21. Vulnerability Management.

Okta performs vulnerability scans at least quarterly on its (1) applications and (2) infrastructure components of its production and development environments. For applications, scans are also performed after any major feature changes or architectural modifications to the Service. Vulnerabilities are ranked using the Common Vulnerability Scoring System, and remediated on a risk basis that considers the types of applications and infrastructure systems on which they are found. Okta installs medium, high, and critical security patches for all components in its production and development environments as soon as commercially reasonable.

22. Penetration Testing.

Okta engages third parties to conduct annual penetration tests of the Service and issue a report of their findings, including confirmation that past findings have been remediated ("**Testing Report**"). Reports from Okta's then-current Testing Report, together with applicable remediation plans, are available to a customer upon its written request. Additionally, Okta's internal penetration testers regularly perform tests of the Service's production infrastructure and application source code.

23. Change and Configuration Management.

Okta maintains policies and procedures for managing changes to production systems, applications, and databases. Such policies and procedures include:

a) A process for documenting, testing and approving the promotion of changes into production;

b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and

c) A process for Okta to perform security assessments of changes into production.

24. Intrusion Detection & Performance Assurance.

Okta implements intrusion, detection, and prevention controls to monitor the Service generally for unauthorized intrusions using traffic and activity-based monitoring systems, and may analyze and share data, such as data collected by Users' web browsers (for example, device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) and authentication event data (collectively, "Threat Information") for security purposes, including to detect compromised browsers and to help customers detect fraudulent authentications, and to ensure that the Service functions properly. For clarity, Threat Information: (1) is only shared if it is derived from evidenced unauthorized attempt(s) to access and/or use the Service; and (2) does not constitute Customer Data.

25. Availability Incident Management.

Okta typically notifies customers of significant system incidents by email to the listed admin contact(s) for the Service, and for availability incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Okta's response.

26. Security Breach Management.

a) Incident Response Plan: Okta has in place a security incident response plan ("IRP") that includes procedures to be followed in the event of any breach of Okta's security that results in the unauthorized disclosure of Customer Data by Okta or its agents, of which Okta becomes aware ("Security Breach"). Okta's IRP addresses the following areas:

   i. Roles and responsibilities: formation of an internal incident response team with a response leader;

   ii. Investigation: assessing the risk the incident poses and determining who may be affected;

   iii. Communication: internal reporting as well as a notification process in the event of a Security Breach;

   iv. Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and

   v. Audit: conducting and documenting a root cause analysis and remediation plan.

b) Notification: Upon its confirmation of a Security Breach, Okta notifies impacted customers to the extent permitted by applicable law, law enforcement directive or regulatory request. Notice shall be sent in accordance with the "Notices" section of an impacted customer's agreement and/or to the listed admin contact(s) for the Service. Okta cooperates with an impacted customer's reasonable request for information regarding such Security Breach, and Okta provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.

c) Remediation: In the event of a Security Breach, Okta shall, at its own expense, (i) investigate the actual or suspected Security Breach, (ii) provide any affected customer with a remediation plan to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents, (iii) remediate the effects of the Security Breach in accordance with such remediation plan, and (iv) reasonably cooperate with any affected customer and any law enforcement or regulatory official investigating such Security Breach.

27. Logs.

Okta records activity in information systems containing or use electronic information, such as logins, connection attempts, privileged User access and actions, along with the source, date, time, and other relevant information for such activities. Okta (i) backs-up logs daily, (ii) implements commercially reasonable measures to protect such logs from unauthorized modification or erasure, and (iii) retains such logs in compliance with Okta's data retention policy. If there is suspicion of inappropriate access to the online Service, Okta may have the ability to provide customers log entry records to assist in forensic analysis. This service, if made available, will be provided to customers on a time-and-materials basis. A customer may access its own organization's system logs via the Okta Admin Console within the Service.

28. Free Trials and Limited Early Access.

Free Trials and subscriptions or features labeled 'Limited Early Access' or 'Early Access' may employ lesser or different privacy and security measures than those present in the Service. Customers should not use Free Trials and subscriptions or features labeled 'Limited Early Access' or 'Early Access' to process personal data contained within Customer Data or other data that is subject to legal or regulatory compliance requirements.

29. Supplemental Provisions Regarding the California Consumer Privacy Act ("CCPA").

Okta processes the data derived from the usage of its products and services, including data regarding service configurations and applications utilized in connection with the hosted Service, support data, operational data, log data and the performance results for the hosted Service ("Usage Data"). Okta may process Usage Data as outlined in the Data Processing Addendum ("DPA"), which is publicly available at https://www.okta.com/trustandcompliance, and for legitimate business purposes, such as to: (i) analyze application usage trends; (ii) detect, investigate, and combat fraud and cyber-attacks; (iii) detect, investigate, and combat security incidents, and other such deceptive, fraudulent or malicious behavior against Okta or its customers, including taking measures to improve Okta's overall security posture; (iv) improve service and product functionality; (v) retain and/or employ another service provider or contractor; and (vi) undertake any other specific business purpose authorized by the Customer. Okta may disclose Usage Data publicly and to other entities, and when doing so, will adhere to any applicable confidentiality obligations. Okta may retain, use, and disclose Usage Data in the normal course of business that is (i) deidentified when disclosed; or (ii) disclosed on an aggregated basis; for example, Okta may make available to the public information showing trends about the general use of the hosted service. For clarity, Usage Data does not include Customer Data. For any personal information, as defined under the CCPA, contained within Usage Data and with respect to which Okta acts as a Service Provider (as defined under the CCPA) ("Personal Information"), then the following sections of the DPA, respectively titled: Definitions, The Parties' Roles, Customer Responsibilities, Processing Purposes, Scope of Processing, Okta's Sub-processors, Liability, GDPR and CCPA Compliance, Customer's Processing Instructions, Personal Data Restrictions, and Deidentified Data shall apply and be interpreted to include Personal Information for such sections. Okta shall permit Customer with the right to take reasonable steps to ensure that Okta uses Personal Information in a manner consistent with its obligations under the CCPA. If Customer receives a consumer request pursuant to the CCPA for Personal Information and requires assistance from Okta, Customer will provide Okta the information necessary for Okta to comply with such request. Notwithstanding the foregoing, Customer expressly authorizes Okta to use such personal information for the legitimate business purposes outlined above and as set forth in the DPA, in accordance with Okta's standard retention policies. Okta owns Usage Data, excluding any Personal Information.

30. Ancillary Processing for Legitimate Business Purposes, Including Under the CCPA.

Okta uses Confidential Information (as defined in the Master Subscription Agreement, available online at https://okta.com/agreements) and Customer Data for the following legitimate business purposes, in accordance with the Master Subscription Agreement, that may be incidental to the provision of the Service. These purposes include: (i) billing and account management; (ii) compensation (*e.g.*, aggregate data for the calculation of compensation due to partners); (iii) internal reporting and business modeling related to the services (*e.g.*, forecasting, revenue analyses, capacity planning, product strategy); (iv) preventing and combating fraud, cyberattacks, or cybersecurity incidents that may impact Okta or its Service and related offerings; (v) improving the Service, including for privacy, security, reliability (including crash and error reporting and diagnostics), availability, and accessibility; (vi) in compliance with applicable obligations, such as for financial reporting and compliance, such as audit requirements; and (vii) aggregation, deidentification, or pseudonymization of Customer Data in connection with the foregoing purposes. For clarity, Okta will use Confidential Information and Customer Data in accordance with its confidentiality obligations set forth in the Master Subscription Agreement.