SECURITY & PRIVACY DOCUMENTATION FOR OKTA REGULATED MODERATE CLOUD[1]

(last updated December 23, 2022)

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, including data submitted by customers to our online service ("Customer Data").

Covered Services

This documentation describes the security-related and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to, the Okta online services branded as the Okta Regulated Moderate Cloud[2] (hereinafter, the "Okta Regulated Moderate Cloud"). For avoidance of doubt, the Service and this documentation does not apply to Professional Services, Support Services, Non-Okta Applications, Free Trials or training services made available by Okta, as those terms are defined in Okta's Master Subscription Agreement, which is publicly available at https://okta.com/agreements ("Master Subscription Agreement").

Customer Eligibility

The Okta Regulated Moderate Cloud is only available to: (1) U.S. government customers (federal, state, local, tribal, territorial, Federally-Funded Research and Development Centers (FFRDCs) or lab entities), (2) government contractors, subcontractors and cloud service providers leveraging the Okta Regulated Moderate Cloud, and (3) entities that need to meet certain U.S. government regulations and requirements (e.g., banking, healthcare, financial services).

Authorization to Operate

As of the date this documentation was last updated, the Okta Regulated Moderate Cloud has been authorized at the FedRAMP Moderate Baseline and is listed on the FedRAMP Marketplace (https://marketplace.fedramp.gov) where a current list of Okta's authorizations to operate is available. In addition, the Okta Regulated Moderate Cloud has a Provisional Authorization (PA) at U.S. Department of Defense Impact Level 2 (IL2) via reciprocity (https://www.doncio.navy.mil/FileHandler.ashx?id=13641).

Additional Customer Data Requirements

Customers may not submit Customer Data to the Okta Regulated Moderate Cloud that is either (1) subject to International Traffic in Arms Regulations (ITAR) or (2) classified data. A customer will be responsible for all sanitization costs incurred by Okta if the customer introduces data subject to ITAR or classified data into the Okta Regulated Moderate Cloud, and such liability of the customer shall be exempt from any limitation of liability set forth in the customer's agreement.

Architecture, Data Segregation, and Data Processing

The Service is operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The Okta architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs," and allows the use of customer and user 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

---

[1] "Okta Regulated Moderate Cloud" was previously named "Okta Regulated Community Cloud" and may appear as such on certain order documents.

[2] The Okta online services currently in scope for the Okta Regulated Moderate Cloud are Single Sign-On, Adaptive Multi-Factor Authentication, Mobility Management, Lifecycle Management, Universal Directory, API Access Management, Directory Integration, Inbound Federation, and Social Authentication (collectively, the "Service").

chain of processing activities by Okta and its sub-processors.

Retrieval of Customer Data

Upon request by a customer made prior to the effective date of termination 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 an industry standard format. 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 deletion of Customer's unique instance of the Service. 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. Additionally, during the term of the agreement, Customer may extract Customer Data from the Okta Service using Okta's standard functionality.

Security Controls

The 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.

Information Security Management Program ("ISMP")

Okta maintains a comprehensive information security management program that contains 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 ISMP is documented and updated based on changes in legal and regulatory requirements related to privacy and data security practices and industry standards applicable to the Service.

Okta's ISMP is designed to:

- Protect the integrity, availability, and prevent the unauthorized disclosure by Okta or its agents, of Customer Data in Okta's possession or control;
- Protect against any anticipated threats or hazards to the integrity, and availability, and prevention of unauthorized disclosure of Customer Data by Okta or its agents;
- Protect against unauthorized access, use, alteration, or destruction of Customer Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data; and
- Safeguard information as set forth in any local, state or federal regulations by which Okta may be regulated.

1. **Security Standards**. Okta's ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing includes:
   a) Internal risk assessments;
   b) ISO 27001, 27002, 27017 and 27018 certifications;
   c) NIST guidance; and
   c) SOC2 Type II (or successor standard) audits annually performed by accredited third-party auditors ("Audit Report").

2. **Security Audit Report**. Okta provides its customers, upon their request, with a copy of Okta's then-current Audit Report, including information as to whether the Security Audit revealed any material findings in the Service; and if so, the nature of each finding discovered.

3. **Assigned Security Responsibility**. Okta assigns responsibility for the development, implementation, and maintenance of its Information Security Management Program, including:

   a) Designating a security official with overall responsibility; and

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

4. **Relationship with Sub-processors**. Okta conducts reasonable due diligence and security assessments of sub- processors engaged by Okta in the storing and/or processing of Customer Data ("Sub-processors"), and enters into agreements with Sub-processors that contain provisions similar to or more stringent than those provided for in this security and privacy documentation.

5. **Background Check**. Okta performs background checks on any employees who are to perform material aspects of the Service or have access to Customer Data.

6. **Security Policy, Confidentiality**. Okta requires all personnel to acknowledge in writing, at the time of hire, that they will comply with the ISMP and protect all Customer Data at all times.

7. **Privacy & Security Awareness and Training**. Okta has annual, mandatory privacy awareness and training programs for all Okta personnel that address their obligations related to the processing of personal data that is contained within Customer Data. Okta has annual, mandatory security awareness and training programs for all Okta personnel that address their implementation of and compliance with the ISMP.

8. **Disciplinary Policy and Process**. Okta maintains a disciplinary policy and process in the event Okta personnel violate the ISMP.

9. **Access Controls**. Okta has in place policies, procedures, and logical controls that are designed:

    a) To limit access to its information systems and the facility or 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 on a timely basis in the event of a change in job responsibilities or job status. Okta institutes:

        a. Controls to ensure that only those Okta personnel with an actual need-to-know will have access to any Customer Data;

        b. Controls to ensure that all Okta personnel who are granted access to any Customer Data are based on least-privilege principles;

        c. Controls to require that user identifiers (User IDs) shall be unique and readily identify Okta person to whom it is assigned, and no shared or group User IDs shall be used for Okta personnel access to any Customer Data;

        d. Password and other strong authentication controls that are made available to Okta customers, so that customers can configure the Service to be in compliance with NIST guidance addressing locking out, uniqueness, reset, expiration, termination after a period of inactivity, password reuse limitations, length, expiration, and the number of invalid login requests before locking out a user;

        e. Periodic (no less than quarterly) access reviews to ensure that only those Okta personnel with access to Customer Data still require it.

10. **Physical and Environmental Security**. Okta maintains controls that provide reasonable assurance that access to physical servers at the production data center 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 monitor and control 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.

11. **Data Encryption.**

    a) Encryption of Transmitted Data: Okta uses Internet-industry-standard secure encryption methods designed to encrypt communications between its server(s) and the customer browser(s), and between its servers and customer's server(s).

    b) Encryption of At-Rest Data: Okta uses Internet-industry standard secure encryption methods to protect stored Customer Data at rest. Such information is stored on server(s) that are not accessible from the Internet.

    c) Encryption of Backups: All offsite backups are encrypted. Okta uses disk storage that is encrypted at rest.

12. **Disaster Recovery**. Okta maintains policies and procedures for responding to an emergency or a force majeure event that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

    a) Data Backups: A policy for performing periodic backups of production file systems and databases to meet the Recovery Point Objective described below;

b) Disaster Recovery: A formal disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested on a regular basis, currently four times a year;

c) RPO / RTO: Recovery Point Objective is no more than 1 hour and Recovery Time Objective is no more than 24 hours;

d) Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

13. 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 Open Web Application Security Project Top 10 and SANS Top 20 Critical Security Controls; and

b) Training: Okta provides employees responsible for secure application design, development, configuration, testing, and deployment appropriate (based on role) training by the security team regarding Okta's secure application development practices.

14. 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.

15. Data Integrity and Management. Okta maintains policies that ensure the following:

a) Segregation of Data: The Service includes logical controls, including encryption, to segregate each customer's Customer Data from that of other customers; and

b) Backup & Archival Copying: Okta performs full backups of the database(s) containing Customer Data no less than once per day and archival storage on no less than a weekly basis on secure server(s) or on other commercially acceptable secure media.

16. Vulnerability Management. Okta maintains security measures to monitor the network and production systems, including error logs on servers, disks and security events for any potential problems. Such measures include:

a) Infrastructure Scans: Okta performs vulnerability scans, no less than quarterly, on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis. Okta installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;

b) Application Scans: Okta performs application scans no less than quarterly (as well as after making any major feature change or architectural modification to the Service). Vulnerabilities are remediated on a risk basis. Okta installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;

c) External Application Vulnerability Assessments: Okta engages third parties to perform network vulnerability assessments and penetration testing on an annual basis ("Vulnerability Assessment"). Reports from Okta's then-current Vulnerability Assessment, together with any applicable remediation plans, will be made available to customers on written request.

Vulnerabilities are remediated on a risk basis. Okta installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible.

17. 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.

18. Secure Deletion. Okta maintains policies and procedures regarding the deletion of Customer Data in compliance with applicable NIST guidance and data protection laws, taking into account available technology so that Customer Data cannot be practicably read or reconstructed. Customer Data is deleted using secure deletion methods including digital shredding of encryption keys and hardware destruction in accordance with NIST SP 800-88 guidelines.

19. Intrusion Detection & Performance Assurance. Okta monitors 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.

20. **Incident Management**. Okta has in place a security incident response plan that includes procedures to be followed in the event of any unauthorized disclosure of Customer Data by Okta or its agents of which Okta becomes aware to the extent permitted by law (such unauthorized disclosure defined herein as a "Security Breach"). The procedures in Okta's security incident response plan include:

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

b) Investigation: assessing the risk the incident poses and determining who may be affected;

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

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

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

Okta publishes system status information on the Okta Trust website, at https://trust.okta.com. Okta typically notifies customers of significant system incidents by email to the listed admin contact, 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.

21. **Security Breach Management**.

a) Notification: In the event of a Security Breach, Okta notifies impacted customers of such Security Breach. 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.

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

22. **Logs.** Okta provides procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports. Okta (i) backs-up logs on a daily basis, (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 Service, Okta has the ability to provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis.

23. **Communications with Administrators.** Separate from and as a complement to the Service, we may provide Okta administrator users ("Admins") access to Okta help and support communities, or communicate with Admins from time to time, including to send announcements and details about our products, services, or other relevant information that Admins' organizations may find useful. Admins who do not want to receive such communications on behalf of their organizations may, for the Service offerings branded as Okta, update their communications preferences by visiting our subscription center, which is available through their admin panel. Admins may also opt-out of non-transactional emails through the Okta Subscription Center, available at https://pages.okta.com/Subscription-Center.html.

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

25. **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 (which is publicly available at https://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 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, 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 of the Data Protection Addendum ("DPA") 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.

26. **Ancillary Processing for Legitimate Business Purposes, Including Under the CCPA.** Okta uses Confidential Information (as defined in the Master Subscription Agreement) 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, 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.