OKTA WORKFLOWS EARLY ADOPTER PROGRAM: TERMS OF SERVICE

These Terms of Service ("Terms of Service") are between Okta, Inc. ("Okta") and the entity (hereinafter "Customer") identified in the applicable ordering document or sign-up page ("Order Form") by which this Agreement is governed. These Terms of Service and the Order Form are collectively referred to hereinafter as the "Agreement". Capitalized terms used in these Terms of Service not otherwise defined herein have the meanings given to them in the Order Form, as applicable. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) the applicable Order Form, (2) this Agreement and (3) any documentation related to Okta's performance under this Agreement (collectively, the "Documentation").

1. SERVICES OFFERING

(a) Access Grant. Upon Customer's execution or acceptance of the applicable Order Form and payment of all required fees therein if applicable, Okta grants Customer the right to access and use the Okta Workflows Early Adopter Program software and services (collectively, the "Services") ordered by Customer in such Order Form solely for Customer's internal business purposes, subject to the terms set forth in this Agreement and in accordance with the Documentation made available by Okta. This right is non-transferable and non-exclusive. Okta reserves the right to modify or improve portions of the Services so long as Customer's access and use of the Services is not materially adversely affected.

(b) Other Software. To the extent Okta provides Customer any software (collectively, the "Software"), Okta grants to Customer a limited, revocable, non-exclusive, non-transferable and non-sublicensable license to install, access, and use such Software solely in connection with Customer's access and use of the Services in accordance with this Agreement and the Documentation made available by Okta. Customer will promptly uninstall and destroy all copies of such Software at the end of the applicable Subscription Term (defined below) for the Services, upon termination of the Agreement, or upon Okta's request, whichever is sooner.

(c) Necessary Equipment. Other than as may be provided by Okta in its discretion, Customer will be solely responsible, at Customer's expense, for acquiring, installing, and maintaining all connectivity equipment, hardware, third party software, and other equipment as may be necessary to connect to, access and use the Services. Customer will comply with Okta's then-current minimum hardware, equipment, and infrastructure requirements for access to and use of the Services that may be disclosed to Customer by Okta.

(d) Restrictions on Use. In no event will Customer: (i) reverse engineer, disassemble, decompile or otherwise attempt to discover the source code or underlying trade secrets, ideas, or algorithms of any of the software comprising any part of the Services; (ii) lease, distribute, license, sell or otherwise commercially exploit any of the Services or make the Services

available to a third party other than as contemplated in this Agreement and/or the Documentation, including but not limited to using the Services for timesharing, service bureau, or other similar purposes; (iii) use the Services on behalf of any third parties; (iv) tamper with other customer accounts of Okta; (v) attempt to gain unauthorized access to the Services or its related systems or networks; (vi) access or use the Service for the purpose of developing a competing product or service; (vii) enter any data into the Services that is subject to the General Data Protection Regulation (i.e., the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) or whereby the provision of such data is otherwise unlawful; (viii) permit anyone else, to engage, directly or indirectly, in any of the activities described in the foregoing subparts (i) through (vii). All the limitations and restrictions on use of the Services in this Agreement will also apply to any Software and Documentation that is part of or provided through the Services (together with the Services and Confidential Information (defined below), collectively, the "Okta Materials"). Okta may restrict or prohibit use of or access to the Services if Customer fails to make payment of fees when due or Okta reasonably suspects that any use or access of the Services is or may be in breach of this Agreement.

(e) Customer Obligations. Customer will: (i) provide Okta with all information and assistance required to provide the Services and enable Customer's use of the Services; (ii) immediately notify Okta of any unauthorized use, copying, distribution, or other suspected security breach in connection with the Services; (iii) not submit any electronic data to the Okta online service ("Customer Data") that is illegal, immoral, obscene, threatening, libelous, otherwise unlawful or tortious, otherwise protected by any intellectual property or proprietary right of any third party, or for which it does not own or has not procured sufficient license, right, consent and permission to copy, disclose, store, broadcast, transmit, or otherwise use in connection with the Services and this Agreement; (iv) be responsible for all activity that occurs in Customer's or its users' accounts (and any transactions completed under Customer's accounts will be deemed to have been lawfully completed by Customer); and (v) be responsible for ensuring that it obtains all consents, permissions, and licenses for any and all Customer Data that is owned or controlled by third parties that Customer copies, discloses, stores, transmits, broadcasts or otherwise uses in connection with the Services.

2. PAYMENT

(a) Fees. Customer shall pay Okta the fees set forth in the applicable Order Form ("Fees") in accordance with this Agreement and the Order Form. If not otherwise specified on an Order Form, Fees will be due within thirty (30) days of date of invoice. Except as otherwise specifically provided in this Agreement, all Fees paid and payable to Okta hereunder are non-cancelable and non-refundable. If Customer fails to pay any amounts due under this Agreement by the due date, in addition to any other rights or remedies it may have under this Agreement or by matter of law, (i) Okta reserves the right to suspend the Services upon thirty (30) days written notice, until such amounts are paid in full, and (ii) Okta will have the right to charge interest at a rate equal to the lesser of one and one-half percent (1.5%) per month or the maximum rate

permitted by applicable law until Customer pays all amounts due; provided that Okta will not exercise its right to charge interest if the applicable charges are under reasonable and good faith dispute and Customer is cooperating diligently to resolve the issue.

(b) Taxes. Fees do not include any local, state, federal or foreign taxes, levies, duties or similar governmental assessments of any nature, including value-added, use or withholding taxes (collectively, "Taxes"). Customer is responsible for paying all Taxes associated with its purchases hereunder (excluding taxes based on Okta's net income or property) unless Customer provides Okta with a valid tax exemption certificate authorized by the appropriate taxing authority. The limitations set forth in Section 6(b) shall not apply to Customer's payment obligations under Section 6(a).

3. TERM; TERMINATION

(a) Term. The subscription period for the Services will be specified in the applicable Order Form, and if none is specified therein, then it will be for the length of time for which Customer has paid the applicable fees, and if no fees have been paid and no subscription period has been specified in the applicable Order Form, then it will be for as long as Okta makes the Early Adopter Program available (the "Subscription Term").

(b) Termination. Either party may terminate this Agreement by written notice to the other party in the event that (i) such other party materially breaches this Agreement and does not cure such breach within thirty (30) days of such notice, or (ii) immediately in the event the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. Upon any termination for cause by Customer pursuant to this section, Okta will refund Customer a pro-rata portion of any prepaid fees that cover the remainder of the applicable Order Form Subscription Term after the effective date of termination. If no fees have paid by Customer, then Okta may terminate this Agreement at any time.

(c) Suspension. Okta may suspend the Services: (a) if Okta considers it necessary to prevent or terminate any actual or suspected use of the Services in violation of this Agreement; or (b) upon notice to Customer if (i) Customer commits a material breach of this Agreement, (ii) Okta reasonably determines that Customer's use of the Services is in excess of the license metrics paid for by Customer in the Order Form, or (iii) if there is a threat to the security and integrity of the hosted environment for the Services. Suspension of Services will be without prejudice to any rights or liabilities accruing before or during the suspension, including Customer's obligation to pay fees.

(d) Effect of Termination. Upon expiration or termination of this Agreement for any reason: (i) any fees, expenses and other amounts accrued and owed to Okta prior to termination or expiration of this Agreement will be immediately due and payable; (ii) all Customer access to the

Services and licenses granted will immediately terminate and Customer shall no longer use the Services; (iii) Okta will have no obligation to maintain any Customer Data stored on behalf of Customer or to forward any Customer Data to any third party; (iv) at Okta's written request, Customer shall certify to Okta the return or destruction of the Software; (v) and within a commercially-reasonable time frame, Okta shall delete any Customer Data of Customer stored within the Services.

(e) Survival. The following Sections will survive termination of this Agreement: the second sentence of 1(b), 1(d), and 2 through 11.

4. CONFIDENTIAL INFORMATION

For the purposes of this Agreement, "Confidential Information" means any information disclosed by Okta to Customer or its users, or any Okta information, data, Software, or other materials that, under the circumstances of disclosure, would be reasonably understood to be considered confidential, including technical data, trade secrets, know-how, research, inventions, processes, designs, drawings, marketing plans, financial information, including but not limited to the Okta Materials. Customer will: (i) hold in strict confidence all Confidential Information; (ii) use the Confidential Information only to perform or to exercise its rights under this Agreement; and (iii) not transfer, display, convey or otherwise disclose or make available such Confidential Information to any person or entity except to the directors, officers, employees, agents, contractors, accountants, auditors and legal and financial advisors of Customer who need to know such Confidential Information, who are under confidentiality obligations substantially similar as those set forth hereunder, and whose handling and treatment of the Confidential Information in accordance with this Agreement is Customer's full responsibility. Customer will use at least the same degree of care to protect the Confidential Information as it uses to protect its own confidential information of like nature, but Customer will use at least reasonable care. Customer may disclose the Confidential Information in response to a valid court order, law, rule, regulation, or other governmental action provided that (x) Customer notifies Okta in writing prior to disclosure of the information in order to provide Okta a reasonable opportunity to obtain a protective order, and (y) Customer assists Okta in any attempt to limit or prevent the disclosure of the Confidential Information. Customer will promptly notify Okta in the event of any unauthorized use or disclosure of the Confidential Information. Customer agrees that Okta may have no adequate remedy at law if there is a breach or threatened breach of this Section 4 and, accordingly, that Okta will be entitled to injunctive or other equitable relief to prevent or remedy such a breach in addition to any legal remedies available to Okta. The obligations in this Agreement with respect to Confidential Information will not apply to any information that would otherwise constitute Confidential Information but that which: (i) is publicly known and made generally available in the public domain without breach of any obligation of confidentiality or restriction on disclosure; or (ii) is in the possession of Customer without breach of any obligation of confidentiality or restriction on disclosure at the time of disclosure by Okta.

Okta agrees to make commercially-reasonable efforts to maintain the confidentiality of Customer Data, in accordance with the Security & Privacy Documentation attached as Appendix 3. The parties agree that Okta may transmit Customer Data to sub-processors in order to provide the Services.

5. OWNERSHIP

Okta will own all intellectual property and other rights in and to the Okta Materials. Unless explicitly stated herein, nothing in this Agreement will be construed as conferring any right or license to such rights, whether by estoppel, implication or otherwise, and Customer acknowledges that it has no ownership interest in the Okta Materials, or any derivatives, modifications, upgrades, updates, new versions, fixes, improvements or enhancements thereof or thereto. Customer hereby assigns to Okta any rights, title and interest, including all intellectual property rights, in any feedback, derivative works, modifications, enhancements, or improvements related to the Okta Materials.

6. AVAILABILITY ASSURANCES, WARRANTIES, AND DISCLAIMER

(a) Okta Assurances. Okta shall make the online Services available to Customer in accordance with: (i) the Service Level Agreement set forth below, in Appendix 2; and (ii) the Security & Privacy Documentation set forth below, in Appendix 3.

(b) Customer Warranties. Customer represents and warrants that (i) it has the full corporate power and authority to enter into this Agreement and perform its obligations hereunder; (ii) it has the necessary rights to enter into this Agreement and perform its obligations hereunder; (iii) this Agreement is a binding obligation upon it and, when executed by both parties, is enforceable in accordance with its terms; (iv) it will comply with all applicable laws, rules and regulations in the course of performing its obligations and exercising its rights under this Agreement; and (v) any Customer Data provided to Okta or otherwise used by either party in connection with this Agreement will not infringe, misappropriate or otherwise violate any right of any third party.

(c) Disclaimer. ALL SERVICES, SOFTWARE AND OTHER OKTA MATERIALS PROVIDED BY OKTA ARE PROVIDED TO CUSTOMER “AS-IS” AND OKTA MAKES NO, AND DISCLAIMS ALL, REPRESENTATIONS AND WARRANTIES, AND CONDITIONS, ORAL OR WRITTEN, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS AGREEMENT, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE. OKTA DOES NOT REPRESENT OR WARRANT THAT THE SERVICES WILL BE DELIVERED FREE OF ANY INTERRUPTIONS, DELAYS, OMISSIONS OR ERRORS OR IN A SECURE MANNER. THE SERVICES MAY BE SUBJECT TO LIMITATIONS, DELAY AND OTHER PROBLEMS INHERENT IN THE USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS. OKTA IS NOT RESPONSIBLE FOR

ANY DELAYS, DELIVERY FAILURES, OR ANY LOSS OF DATA OR DAMAGES RESULTING THEREFROM. THE SERVICES MAY CONTAIN INDEPENDENT THIRD PARTY PRODUCTS AND RELY ON THEM TO PERFORM CERTAIN FUNCTIONALITY IN CONNECTION WITH THE SERVICES. OKTA MAKES NO WARRANTY AS TO THE OPERATION OF ANY THIRD PARTY PRODUCTS OR THE ACCURACY OF ANY THIRD PARTY INFORMATION. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY OKTA OR ITS AUTHORIZED REPRESENTATIVES WILL CREATE ANY WARRANTY.

7. INDEMNIFICATION

Customer will defend, indemnify, and hold harmless Okta, its affiliates, subsidiaries, and parent companies, together with each of their respective officers, directors, members, employees, agents, contractors, representatives, successors and assigns (each, a “Okta Indemnitee”) against any and all losses, damages, liabilities, judgments, awards, penalties, interest, fines, costs, fees or expenses of whatever kind, including reasonable attorneys’ fees, professional fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, which are incurred by any Okta Indemnitee arising out of any third party claim, demand, allegation, investigation, or other proceeding made in connection with or otherwise related to Customer’s breach of any representation, warranty or covenant in this Agreement.

8. LIMITATION OF LIABILITY

(a) Customer Responsibility. The failure or delay of Okta in its performance of its obligations under the Agreement is excused to the extent such failure is a result of: (i) any act or omission of Customer or any entity or individual acting on Customer’s behalf, including Customer’s failure to perform (or cause to be performed) its obligations hereunder; (ii) unavailability of Customer’s materials or systems, including those provided by third parties; (iii) the reliance of Okta on instructions, authorizations, approvals or other information from Customer’s representative(s); or (iv) any act or omission of a third party not under the control of Okta. Okta will use commercially reasonable efforts to provide the Services notwithstanding such circumstances, and Customer will reimburse Okta for any additional charges and expenses incurred as a result thereof.

(b) Limitation and Disclaimer. IN NO EVENT WILL OKTA (OR ITS SUPPLIERS OR AFFILIATES) BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR ANY PUNITIVE, SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, LOST PROFIT OR OTHER SIMILAR DAMAGES ARISING OUT OF, OR IN CONNECTION WITH, THIS AGREEMENT, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL OKTA’S TOTAL AGGREGATE LIABILITY FOR DAMAGES OF ANY NATURE UNDER OR IN CONNECTION WITH THIS AGREEMENT, REGARDLESS OF THE FORM OF THE ACTION OR THE THEORY OF RECOVERY, EXCEED THE AGGREGATE AMOUNT ACTUALLY PAID BY CUSTOMER TO OKTA UNDER THE

APPLICABLE ORDER DURING THE 12 MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY. IN NO EVENT WILL OKTA HAVE ANY LIABILITY ARISING OUT ANY OF CUSTOMER Data PROVIDED TO OKTA IN CONNECTION WITH THE SERVICES HEREUNDER.

9. MANDATORY ARBITRATION

The parties consent to arbitrate any claim, dispute or controversy (each, a “Claim”) arising out of or relating to this Agreement or the relationships among the parties hereto through binding arbitration administered by the American Arbitration Association (”AAA”). The parties will notify each other in writing of any Claim within 30 days of when it arises. Notice to Okta will be sent to 100 First Street, San Francisco, California 94105, Attention: Legal. The parties further agree: (i) to attempt informal resolution of the Claim prior to any demand for arbitration; (ii) that any arbitration will occur in San Francisco County, California; (iii) that arbitration will be conducted confidentially by a single arbitrator in accordance with the Rules of the American Arbitration Association; and (iv) that the state or federal courts in San Francisco County, California have exclusive jurisdiction over any appeals of an arbitration award. The arbitrator, and not any federal, state, or local court, will have exclusive authority to resolve any dispute relating to the interpretation, applicability, unconscionability, arbitrability, enforceability, or formation of this Agreement including any claim that all or any part of the Agreement is void or voidable. However, the preceding sentence will not apply to the Section entitled “Class Action Waiver” immediately below. Any dispute between the parties will be governed by this Agreement and the laws of the State of California and applicable United States law, without giving effect to any conflict of laws principles that may provide for the application of the law of another jurisdiction.

10. EXPORT CONTROLS

Customer will comply with all export and re-export restrictions and regulations imposed by the government of the United States and other relevant countries or regions (”Export Restrictions”). Customer will not transfer, directly or indirectly, any restricted Software or technical data received hereunder or the direct product of such data, to any country or region identified as an embargoed destination or country in the Export Restrictions, unless prior written authorization is obtained from Okta and each appropriate United States or other government agencies.

11. GENERAL

This Agreement sets forth the entire agreement and understanding between the parties hereto with respect to the subject matter hereof and, supersedes and merges all prior oral and written agreements, discussions and understandings between the parties with respect to the subject matter hereof. Any amendment to this Agreement must be in writing and signed by the authorized representatives of the parties. Except for payment obligations, each party will be excused from performance of its obligations under this Agreement if such a failure to perform

results from acts beyond its reasonable control. Customer may not assign this Agreement, by merger (including operation of law), transfer of equity, other change of control or otherwise, and any attempt to do so is null, void and of no effect. All notices required under this Agreement will be in writing and sent by express mail or other overnight delivery service providing receipt of delivery to the address set forth in the Order, with notice effective upon delivery. The parties hereto are independent contractors. Nothing in this Agreement will be deemed to create an agency, employment, partnership, fiduciary, or joint venture relationship between the parties. No waiver under this Agreement will be valid or binding unless set forth in writing and duly executed by the party against whom enforcement of such waiver is sought. Any delay or forbearance by either party in exercising any right hereunder will not be deemed a waiver of that right. If any portion of this Agreement is held invalid, illegal or unenforceable, such determination will not impair the enforceability of the remaining terms and provisions herein.

12. OKTA SUPPORT SERVICES

Okta will provide support services to Customer in accordance with the support terms set forth in Appendix 1 to these Terms of Service.

APPENDIX 1: SUPPORT TERMS

Okta Early Adopter Program Support
("Support Services")

Okta Early Adopter Program Support terms are subject to the Terms of Service, and capitalized terms not defined here will have the meaning specified (if applicable) in the Terms of Service.

Okta Support Offerings

Priority Levels:
In the event that a Services-affecting issue is detected by Okta or reported by Customer, Okta shall, in its reasonable discretion, categorize the Priority Level pursuant to the criteria below.

Priority Level	Description	Examples
1	A Services failure or severe degradation. Customer is unable to access any business resources.	Services are down and not accessible by users; Services are slowed to such a degree that multiple users cannot log in, resulting in consistent "page not found errors" or similar.
2	A partial Services failure or mild degradation. Customer is able to access some but not all business resources.	Customer lacks write-access to the administrative feature of the Services (excluding regularly scheduled Service upgrades); the Services are accessible but return periodic errors to multiple users, preventing reliable access to infrastructure.
3	Minor Services impact. Customer is able to access almost all business resources.	All users are unable to authenticate to non-critical infrastructure such as development servers; one user is not able to access critical infrastructure (for example, due to a client application configuration issue).
4	Services feature enhancement. Customer is able to access all business resources and is requesting a Services feature enhancement.	Services feature enhancement requests.

Response Times:
Okta will use reasonable efforts to adhere to the following response times below:

Response Time for the Services
(Support hours are 8 a.m. to 8 p.m. Pacific Time)

Priority Level	First Response	Subsequent Updates
1	4 hours	12 hours
2	12 hours	24 hours
3	Next business day	36 hours from first response
4	Next business day	36 hours from first response

Early Adopter Program Support Details:
Early Adopter Program Support provides the following benefits to the Customer:

Benefit	Details
Customer Support	• Customer may contact Okta Support via http://support.okta.com or phone at 1-800-219-0964 ▪ Support requests are responded to within the timeframes defined in the Service Level Agreement during the support hours above.

APPENDIX 2: SERVICE LEVEL AGREEMENT

This Service Level Agreement ("SLA") is provided under and forms an Appendix to the Terms of Service. Capitalized terms used in this SLA that are not defined herein are defined as set forth in the Terms of Service, if applicable.

Service Level Commitment:

The online Services will, subject to the exceptions listed below, be available at least 99% of the time during any full calendar month in Customer's production environment ("Availability Commitment"). The Availability Commitments do not apply to sandbox, beta and other test environments.

The Availability Commitment of the Services for a given month will be calculated as follows (rounded to the nearest one tenth of one percent):

$$\text{Availability \%} = 100\% \times \frac{\text{(Total Minutes in the Month – Total Minutes Unavailable in the Month)}}{\text{Total Minutes in the Month}}$$

The Services will be deemed to be unavailable only if the Services do not respond to HTTPS requests, ("Unavailable").

The Services will not be deemed Unavailable for any downtime or outages relating to: (i) a Customer Outage Event, (ii) equipment, applications, interfaces, integrations, or systems not owned by Okta, or service not offered by Okta or (iii) a Force Majeure Event.

"Customer Outage Event**"** means a period of time in which the Services are not available due to acts, omissions or requests of Customer, including without limitation (a) configuration changes in, or failures of, the Customer end of the network connection, (b) work performed by Okta at Customer's request, (c) Customer's unavailability or untimely response to incidents that require its participation for source identification and/or resolution or (d) Customer's failure to provide Okta with any requested physical or remote access to any Customer facilities, equipment or personnel.

Emergency Maintenance:

Okta may perform emergency maintenance for which Okta will use commercially reasonable efforts to notify Customer at least twenty-four (24) hours in advance. For the avoidance of doubt, if the Services are Unavailable due to emergency maintenance, such Unavailability will be included in the Availability calculation.

Service Level Credits:

For each full calendar month in which Okta fails to meet the Availability Commitment of at least 99.9% (a "Service Level Failure"), Customer shall receive a service level credit equal to an amount determined in accordance with this following schedule ("Service Level Credit"). The Service Level Credit shall be calculated as the applicable percentage outlined below multiplied by the annual subscription fee paid by Customer for the then current annual period divided by twelve (12):

Availability %	**Service Level Credit**
98.5% – 98.99%	5%
97% - 98.49%	10%
< 97%	20%

If required under this SLA, Service Level Credits will be issued to the Customer in the form of monetary payment. The Service Level Credits stated herein are Customer's sole and exclusive remedy (and Okta's sole liability) for any claims in connection with this Service Level Agreement.

Reporting and Confirmation:

Customer may contact Okta to report Services outages via either http://support.okta.com or phone at 1-800-219-0964.

Customer must log an incident within three (3) business days following any time in which the Services are Unavailable, along with the following information, in order for the applicable minutes to be applied towards the Availability % calculation:

(i) The manner in which the Services are not available; and

(ii) The date and time in which the Services first became not available.

Failure to provide such notice will forfeit the right to receive Service Level Credits. Provided such notice is timely given, Unavailable minutes will be calculated from the starting time of the incident until the time the incident is resolved by Okta. Upon receipt of Customer's notification, Okta will verify Customer's report through any available system logs and records.

APPENDIX 3:
SECURITY & PRIVACY DOCUMENTATION FOR WORKFLOWS EARLY ADOPTER PROGRAM

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 Workflows (collectively, the "Service"). Okta may update this documentation from time to time, in order to communicate improvements or other modifications to its security & privacy program.

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

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 comma separated value (.csv) 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 internal risk assessments and NIST guidance.

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 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. **Security Awareness and Training**. Okta has 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 in 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 designed 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 OWASP 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) Back Up/Archival: 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 quarterly vulnerability scans 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 quarterly (as well as after making any major feature change or architectural modification to the Service) application vulnerability scans. 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 Assessment: 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 SP800-88 guidelines.

19. **Intrusion Detection.** Okta monitors the Service generally for unauthorized intrusions using traffic and activity-based monitoring systems. Okta may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to help customers detect fraudulent authentications, and to ensure that the Service functions properly.

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.