OKTA, INC.
SERVICE-SPECIFIC TERMS

These Service-Specific Terms (these "SSTs") govern the use of the Service and supplement the Master Subscription Agreement (or other written or electronic agreement governing Customer's use of the Service) ("Agreement") between Okta and Customer, to which these SSTs are incorporated therein. Capitalized terms used in these SSTs but not otherwise defined herein have the meanings given to them in the Agreement.

By executing an Order Form that references these SSTs, by using the Service, or by otherwise accepting these SSTs, Customer agrees to these SSTs and will use the Service in compliance with them.

Table of Contents:

1. General Terms (last updated November 18, 2025).
2. Cross-over Service-Specific Terms for Okta and Auth0 Services (last updated April 9, 2026).
3. Auth0 Service-Specific Terms (last updated April 1, 2026).
3.1 Adaptive MFA (last updated October 20, 2025).
3.2 Attack Protection Package (last updated November 18, 2025).
3.4 Auth0 for AI Agents add-on SKU (last updated May 14, 2026).
3.5 Client-Initiated Backchannel Authentication ("CIBA Service") (last updated November 18, 2025).
3.6 Enterprise MFA (last updated February 12, 2026).
3.7 Enterprise MFA Factors (last updated August 15, 2025).
3.8 Highly Regulated Identity ("HRI Service") (last updated August 15, 2025).
3.9 Private Performance Burst Azure (last updated December 18, 2025).
3.10 Private Performance Burst Azure International (last updated December 18, 2025).
3.11 Private Performance Burst Geo HA Azure (last updated December 18, 2025).
3.12 Private Performance Burst Geo HA Azure International (last updated December 18, 2025).
3.13 Public Performance Burst (last updated November 18, 2025).
3.14 Token Vault (last updated November 18, 2025).
4. Okta Service-Specific Terms (last updated June 12, 2026).
4.1 Okta for AI Agents (last updated October 26, 2026).
4.2. Okta for AI Agents - Core (last updated October 26, 2026).
4.3. Okta for AI Agents for Okta Customer Identity (last updated October 26, 2026).
5. Okta Digital Workers Service Specific Terms (last updated November 5, 2026).
5.1 Okta Digital Workers (last updated November 5, 2026).

1. General Terms (last updated November 18, 2025).

1.1 Okta may update or modify these SSTs from time to time effective when updated on okta.com/legal.

2. Cross-over Service-Specific Terms for Okta and Auth0 Services (last updated April 9, 2026).

2.1 AI Agent Services (last updated April 9, 2026)

2.1.1 Definitions.

a) "AI" or "Artificial Intelligence" means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

b) "AI Agent" means any AI-driven software, systems, or processes that take autonomous actions on behalf of Customer with little to no human supervision to achieve specific goals, is connected to the Service, and on which Customer uses the Service to manage, govern, secure, authenticate, identify, or take any other action.

c) "AI Agent Service" means any Service or feature, functionality or component of a particular Service that enables, integrates with, or is used to identify, register, govern, manage, secure, authenticate, or take any other action on an AI Agent, including but not limited to Okta for AI Agents and Auth0 for AI Agents.

2.1.2 Customer Responsibility for AI Agents. As between the parties, Customer is fully responsible for all acts, controls, configuration, omissions, and errors of its AI Agents, including compliance with all usage and other restrictions. Any activity conducted by or on behalf of an AI Agent is deemed activity of the Customer for purposes of compliance with the Agreement, these SSTs, and the applicable Order Form.

2.1.3 Monitoring and Usage Verification. Okta may monitor Customer's use of the AI Agent Service. Customer shall not, directly or indirectly: (I) destroy, disable, corrupt, or tamper or interfere with any part of the AI Agent Service, including any monitoring or reporting technology; or (ii) attempt to falsify, undercount, obscure or otherwise manipulate any calculation of Customer's use of the AI Agent Service.

2.1.4 Reasonable Use. Customer shall use commercially reasonable efforts to implement usage limits consistent with any Okta provided guidance, published technical limitations, and industry best practices ("Reasonable Use"). Customer will cooperate with Okta to ensure the secure, efficient, and continuous operation of the AI Agent Service. Usage that, in Okta's reasonable discretion, threatens the stability, security, or availability of Okta's multi-tenant platform for Customer or other customers, or results in a material increase in Okta's costs to provide the AI Agent Service, shall be deemed to be in excess of Reasonable Use and may be subject to additional fees, throttling, or suspension.

2.1.5 Applicability. The terms in this section apply generally to any AI Agent Service. A specific AI Agent Service may have additional terms and conditions as set forth in these SSTs.

3. Auth0 Service-Specific Terms (last updated April 1, 2026).

3.1 Adaptive MFA (last updated October 20, 2025).

3.1.1 Adaptive MFA is only offered as an add-on SKU for Enterprise Plans. Custom Device Remembrance is included in Adaptive MFA.

3.1.2 Adaptive MFA provides Adaptive MFA Enterprise MFA factors, and Adaptive MFA Triggers. SMS for MFA is charged separately by carriers supported by Auth0; details are listed at https://auth0.com/docs/attack-protection, https://auth0.com/docs/multifactor-authentication and https://auth0.com/docs/mfa/adaptive-mfa.

3.1.3 Customer is solely responsible for any diminishment in security posture caused by adjusting their device remembrance time period to a period of time longer than Okta's standard recommended setup.

3.2 Attack Protection Package (last updated November 18, 2025).

3.2.1 Attack Protection Package is only offered as an add-on SKU for Enterprise Plans.

3.2.2 Attack Protection Package enhances attack protection and security measures by increasing Tenant Access Control list beyond core plan entitlements and enabling the Credential Guard, Bot Detection, and Supplemental Signals functionality; additional usage details are listed at https://auth0.com/docs/attack-protection.

3.3 Auth for MCP (last updated May 14, 2026).

3.3.1 Auth for MCP is available for all Auth0 Plans and includes Client ID Metadata (CIMD) Registration and On-Behalf-Of Token Exchange. On-Behalf-Of Token Exchange is subject to RPS limits based on Customer's plan tier.

3.4 Auth0 for AI Agents add-on SKU (last updated May 14, 2026).

3.4.1 Auth0 for AI Agents add-on SKU is only offered for Enterprise and Growth Plans.

3.4.2 Auth0 for AI Agents (i) increases Customer's Token Vault number of connected apps beyond core plan entitlements; (ii) expands notification channels for CIBA flows; and (iii) increases the Customer's On-Behalf-of Token Exchange RPS limit up to the plan's Authentication API RPS limit provided at https://auth0.com/docs/troubleshoot/customer-support/operational-policies/rate-limit-policy/rate-limit-configurations .

3.4.3 For the Auth0 for AI Agents add-on SKU, CIBA includes SMS, Email, Voice, and other notification channels for CIBA flows as updated. SMS is charged separately by carriers supported by Auth0. Details are listed at https://auth0.com/docs/multifactor-authentication.

3.5 Client-Initiated Backchannel Authentication ("CIBA Service") (last updated November 18, 2025).

3.5.1 The CIBA Service is included in Enterprise Plans and only includes notification channels for Auth0 Guardian App and SDK.

3.5.2 Notwithstanding anything to the contrary in the Agreement, Customer may submit to the CIBA Service Customer Data that is considered Regulated Data, solely for Customer's business purposes, provided that Customer agrees: a) to only submit Regulated Data as part of the CIBA Service in accordance with the Documentation, (b) that Regulated Data will not include any government identifiers or Social Security numbers, any payment card or other data subject to the Payment Card Industry Data Security Standard, any other personal data that

is considered "special" or "sensitive" under applicable Laws, or any protected health information subject to the Health Insurance Portability and Accountability Act except as Okta otherwise agrees in writing, and (c) that Customer is solely responsible for ensuring that its use of the CIBA Service in connection with Non-Okta Applications (as defined in the Agreement) complies with all Laws applicable to Customer's services and products.

3.6 **Enterprise MFA (last updated February 12, 2026).**

3.6.1 This Enterprise MFA SKU is an add-on to Auth0 B2B Essentials Growth plan and includes second factor support for Auth0 Guardian, SMS, Email, Voice, webauthN, and other notification channels as updated. SMS is charged separately by carriers supported by Auth0. Details are listed at https://auth0.com/docs/multifactor-authentication.

3.7 **Enterprise MFA Factors (last updated August 15, 2025).**

3.7.1 Enterprise MFA Factors is included in B2C & B2B Professional, as well as all Enterprise Plans.
3.7.2 Enterprise MFA Factors includes second factor support for Auth0 Guardian, SMS, Email, Voice and others as updated. SMS and Voice for MFA are charged separately by carriers supported by Auth0. Details are listed at https://auth0.com/docs/multifactor-authentication.

3.8 **Highly Regulated Identity ("HRI Service") (last updated August 15, 2025).**

3.8.1 HRI Service is only offered as an add-on SKU for Enterprise Plans.
3.8.2 Notwithstanding anything to the contrary in the Agreement, Customer may submit to the HRI Service Customer Data that is considered personal financial data or other similarly regulated personal data, such as bank account numbers (collectively, "Regulated Data"), solely for Customer's business purposes, provided that Customer agrees: a) to only submit Regulated Data as part of the HRI Service in accordance with the Documentation, b) that Regulated Data will not include any government identifiers or Social Security numbers, any payment card or other data subject to the Payment Card Industry Data Security Standard, any other personal data that is considered "special" or "sensitive" under applicable Laws, or any protected health information subject to the Health Insurance Portability and Accountability Act except as Okta otherwise agrees in writing, and c) that Customer is solely responsible for ensuring that its use of the HRI Service in connection with Non-Okta Applications (as defined in the Agreement) complies with all Laws applicable to Customer's services and products.

3.9 **Private Performance Burst Azure (last updated December 18, 2025).**

3.9.1 Private Performance Burst Azure SKU is only available to Enterprise Private Cloud Customers and includes a single geographical deployment of the Private Performance Burst Environment in the United States, Canada, Mexico, or Europe.
3.9.2 This SKU also includes one development environment that provides a low capacity, non-production environment hosted within a single region in the Auth0 dedicated cloud Service, and is intended for development or testing environments only. Customers have no guaranteed RPS in the development environment.
3.9.3 This add-on SKU only extends the Authentication API request limits and does not apply to the Management API or other endpoints that are rate-limited outside the scope of the Authentication API.

3.10 **Private Performance Burst Azure International (last updated December 18, 2025).**

3.10.1 Private Performance Burst Azure International SKU is only available to Enterprise Private Cloud Customers and includes a single geographical deployment of the Private Performance Burst Environment outside of the United States, Canada, Mexico, and Europe.
3.10.2 This SKU also includes one development environment that provides a low capacity, non-production environment hosted within a single region in the Auth0 dedicated cloud Service, and is intended for development or testing environments only. Customers have no guaranteed RPS in the development environment.
3.10.3 This add-on SKU only extends the Authentication API request limits and does not apply to the Management API or other endpoints that are rate-limited outside the scope of the Authentication API.

3.11 **Private Performance Burst Geo HA Azure (last updated December 18, 2025).**

3.11.1 This SKU is an add-on to the Private Performance Burst Azure SKU and allows for a geographically redundant failover to be deployed in the United States, Canada, Mexico, or Europe.
3.11.2 The Performance Multiple subscribed to for this SKU must align with the base deployment subscribed to for the Private Performance Burst Azure SKU.

3.12 **Private Performance Burst Geo HA Azure International (last updated December 18, 2025).**

3.12.1 This SKU is an add-on to the Private Performance Burst Azure International SKU, and allows for a geographically redundant failover to be deployed outside the United States, Canada, Mexico, and Europe.
3.12.2 The Performance Multiple subscribed to for this SKU must align with the base deployment subscribed to for the Private Performance Burst Azure International SKU.

3.13 **Public Performance Burst (last updated November 18, 2025).**

3.13.1 The Public Performance Burst offering is only offered as an add-on SKU for Enterprise Plans that enhances an existing Public Cloud deployment.
3.13.2 This add-on SKU only extends the Authentication API request limits and does NOT apply to the Management API or other endpoints that are rate-limited outside the scope of the Authentication API.

3.14 **Token Vault (last updated November 18, 2025).**

3.14.1 Token Vault is included in all Auth0 plans.
3.14.2 Connected Accounts is a feature of Token Vault.
3.14.3 Connected account deletion only removes the external provider's access and refresh tokens from token vault, but does not automatically revoke tokens from Customer's external provider. Customer is responsible for manually revoking the tokens from Customer's external provider.

4. Okta Service-Specific Terms (last updated October 26, 2026).

4.1 **Okta for AI Agents (last updated October 26, 2026).**

4.1.1 Definitions. The following definitions apply to Okta for AI Agents:
4.1.1.1 "Agentic Identity Services" means the agentic features and functionalities provided under the Okta for AI Agents SKU, which includes but is not limited to Identity Security Posture Management ("ISPM"), Universal Directory, Single Sign-On, API Access Management, Okta Privileged Access, and Access Governance, as further described in the Documentation.
4.1.2 Scope of Use**.** Customer shall use Okta for AI Agents solely to identify, authenticate, register, govern and manage its AI Agents using the Agentic Identity Services, in accordance with these SSTs, the applicable Order Form, the Agreement, and the applicable Documentation and for no other purpose. For clarity, Customer may not use Okta for AI Agents, in whole, or in part, directly or indirectly, to: (i) identify, authenticate, govern or manage any employee, contractor, partner, customer or other human identity for purposes of directly accessing any system, application or other computing resource that is not an AI Agent; or (ii) perform any use cases prohibited in the Documentation.
4.1.3 Licensing**.** Okta for AI Agents is licensed based on the number of Users per Month. For more information, see the Product Subscription Reference Guide. Customer shall not exceed the number of Users per Month specified in the applicable Order Form. In addition, (i) the number of Users per Month purchased may not be decreased during the Term; (ii) additional Users per Month may be added during the then-current Term at the same pricing as that for the pre-existing Users per Month thereunder, prorated for the remainder of the Term in effect at the time the additional Users per Month are added; and (iii) the added Users per Month shall terminate on the same date as the then-current Term.
4.1.4 Service-Specific Terms for Agentic Identity Services**.**
4.1.4.1 Access Governance**.** Access Governance includes three features: Access Requests, Access Certifications, and Reporting.
4.1.4.2 ISPM.
4.1.4.2.1 ISPM Data Storage. As part of Customer's purchase of subscriptions for ISPM, Customer agrees that the primary location for the storage of Customer Data will be at data center(s) located in the region where Customer's cell is located, unless the Customer is a multi-cell tenant, in which case the default primary data center is the EU, but may be in data centers in other regions depending on Customer preference or as required for the Service. In either case, data processing activities may occur in other regions, as described in Okta's 'Sub-Processor Information' documentation at https://www.okta.com/trustandcompliance/.
4.1.4.2.2 ISPM Integration. Customer may integrate ISPM with, or connect ISPM to, other services, applications, or accounts (each, an "ISPM Integration"), which may include Non-Okta Products (as defined in the Agreement). For more information about ISPM Integrations (including any applicable system limits), see the Product Subscription Reference Guide and the applicable Documentation.
4.1.5 Customer Use Only. Notwithstanding anything to the contrary in the Agreement, for purposes of the applicable Order Form, Customer only means Customer and none of Customer's Affiliates, majority or minority owned subsidiaries, parent companies, or any other related entities, whether created through a divestiture or reorganization or acquired by purchase, merger, consolidation or otherwise, shall access or use Okta for AI Agents, including the Agentic Identity Services, and such Services shall not be used for the benefit of (e.g., to identify, authenticate, govern or manage) such entities or for any unrelated third party.
4.1.6 Exclusions. Okta for AI Agents is excluded from: (i) the Canada-Hosted Cell Add-On, the India-Hosted Cell Add-On, and any terms or requirements for these Cell Add-Ons shall not apply to Okta for AI Agents; (ii) any Health Insurance Portability and Accountability Act standards that may be applicable; and (iii) any authorization(s) not yet granted under the FedRAMP program or by the U.S. Department of Defense. Okta for AI Agents is not available in Okta for Government Moderate, Okta for Government High, or Okta for US Military cells.

4.2 **Okta for AI Agents – Core (last updated October 26, 2026).**

4.2.1 Definitions**.** The definitions set forth below only apply to subscriptions for Okta for AI Agents - Core. All capitalized terms used in this section but not defined below shall have the meaning given to them in the Agreement.

4.2.1.1 "Agentic Identity Services - Core" means the agentic features and functionalities provided under the Okta for AI Agents - Core SKU, which includes but is not limited to Universal Directory, Single Sign-On, API Access Management, and Access Governance, as further described in the Documentation.

4.2.2 Scope of Use**.** Customer shall Okta for AI Agents - Core solely to authenticate, govern and manage its AI Agents using the Agentic Identity Services - Core, in accordance with the applicable Order Form, the Customer Agreement, and any applicable Documentation and for no other purpose. For clarity, Customer may not use Okta for AI Agents - Core , including the Agentic Identity Services - Core, in whole, or in part, directly or indirectly, to: (i) authenticate, govern or manage any employee, contractor, partner, customer or other human identity for purposes of directly accessing any system, application or other computing resource that is not an AI Agent; or (ii) perform any use cases prohibited in the Documentation.

4.2.3 Reasonable Use. Customer shall use commercially reasonable efforts to implement usage limits consistent with any Okta provided guidance, published technical limitations, and industry best practices ("Reasonable Use"). Customer will cooperate with Okta to ensure the secure, efficient, and continuous operation of Okta for AI Agents - Core. Usage that, in Okta's reasonable discretion, threatens the stability, security, or availability of Okta's multi-tenant platform for Customer or other customers, or results in a material increase in Okta's costs to provide Okta for AI Agents - Core, shall be deemed to be in excess of Reasonable Use and may be subject to additional fees, throttling, or suspension.

4.2.4 Public Entity Use Only**.** Notwithstanding anything to the contrary in the Agreement, for purposes of the applicable Order Form for the purchase of the Okta for AI Agents – Core SKU, Customer shall mean only the specific governmental department, agency, or office identified in the Order Form for the Okta for AI Agents – Core SKU. This definition excludes all other departments, sub-governmental departments, agencies, branches, political subdivisions, municipalities, or independent statutory bodies within the same jurisdiction.

4.2.5 Licensing**.** Okta for AI Agents - Core is licensed based on the number of Users per Month. For more information, see the Product Subscription Reference Guide. Customer shall not exceed the number of Users per Month specified in the applicable Order Form for the Okta for AI Agents – Core SKU. In addition, (i) the number of Users per Month purchased under the Order Form may not be decreased during the Term; (ii) additional Users per Month may be added during the then-current Term at the same pricing as that for the pre-existing Users per Month thereunder, prorated for the remainder of the Term in effect at the time the additional Users per Month are added; and (iii) the added Users per Month shall terminate on the same date as the then-current Term.

4.2.6 Modifications to Okta for AI Agents - Core SKU. Customer acknowledges and agrees that **Okta Privileged Access, Identity Security Posture Management, Access Governance's Governance Analyzer feature,** and **the LLM-generated summary functionality within the Security Access Reviews feature of Access Governance** are excluded from the purchase of the Okta for AI Agents - Core SKU as these Services and features have not yet received a FedRAMP Moderate, FedRAMP High authorization, and/or DoD Impact Level (IL) authorization . Additionally, any feature included in the standard Okta for AI Agents SKU that has not yet received a FedRAMP Moderate, FedRAMP High, or DoD IL authorization is also excluded. For a current list of such excluded features, please refer to the Okta US Public Sector Limitations or Exceptions documentation at https://support.okta.com/help/s/article/okta-us-public-sector-limitations-or-exceptions?language=en_US, which Okta may update from time to time.

4.2.7 Subscription Renewal**.** Upon expiration of the current Term for Okta for AI Agents - Core, the parties shall engage in commercially reasonable negotiations to renew the subscription. Customer acknowledges and agrees that such renewal shall be subject to Okta's then-current Units of Measure and pricing models at the time of renewal, which may vary from those set forth in the applicable Order Form for the Okta for AI Agents- Core SKU.

4.3 **Okta for AI Agents for Okta Customer Identity (last updated October 26, 2026).**

4.3.1 Definitions. The definitions set forth below only apply to subscriptions for the Okta for AI Agents for Okta Customer Identity SKU. All capitalized terms used in this section but not defined below shall have the meaning given to them in the Agreement.

4.3.1.1 "OCI Agentic Identity Services" means the AI Agent-specific features and functionalities provided under the Okta for AI Agents for Okta Customer Identity SKU, which includes but is not limited to the following Okta Customer Identity features: Universal Directory, Single Sign-On, Agent Registry and Directory, Access Policies, Agent-to-Agent, Cross-App Access, Manual Kill Switch, and End-to-End Auditing, as further described in the Documentation. For the avoidance of doubt, the OCI Agentic Identity Services explicitly excludes Identity Security Posture Management, Okta Privileged Access, and Access Governance.

4.4.2 Scope of Use. Customer shall use Okta for AI Agents for Okta Customer Identity solely to authenticate, govern and manage its AI Agents using the OCI Agentic Identity Services, in accordance with this Order Form, the Customer Agreement, and any applicable Documentation and for no other purpose. For clarity, Customer shall not use Okta for AI Agents for Okta Customer Identity, including the OCI Agentic Identity Services, in whole, or in part, directly or indirectly, to: (i) authenticate, govern or manage any employee, contractor, partner, customer or other human identity for purposes of directly accessing any system, application or other computing resource that is not an AI Agent; or (ii) perform any use cases prohibited in the Documentation.

4.4.3 Responsibility for AI Agents**.** As between the parties, Customer is fully responsible for all acts, controls, configuration, omissions and errors of its AI Agents, including compliance with all usage and other restrictions. Any activity conducted by or on behalf of an AI Agent is deemed activity of the Customer for purposes of compliance with the Agreement and this Order Form.

4.4.4 Monitoring and Usage Verification**.** Okta may monitor Customer's use of Okta for AI Agents for Okta Customer Identity. Customer shall not, directly or indirectly: (i) destroy, disable, corrupt, or tamper or interfere with any part of Okta for AI Agents for Okta Customer Identity, including any monitoring or reporting technology; or (ii) attempt to falsify, undercount, obscure or otherwise manipulate any calculation of Customer's use of Okta for AI Agents for Okta Customer Identity.
4.4.5 Reasonable Use. Customer shall use commercially reasonable efforts to implement usage limits consistent with any Okta provided guidance, published technical limitations, and industry best practices ("Reasonable Use"). Customer will cooperate with Okta to ensure the secure, efficient, and continuous operation of Okta for AI Agents for Okta Customer Identity. Usage that, in Okta's reasonable discretion, threatens the stability, security, or availability of Okta's multi-tenant platform for Customer or other customers, or results in a material increase in Okta's costs to provide Okta for AI Agents for Okta Customer Identity, shall be deemed to be in excess of Reasonable Use and may be subject to additional fees, throttling, or suspension.
4.4.6 Customer Use Only. Notwithstanding anything to the contrary in the Agreement, for purposes of the applicable Order Form, Customer only means Customer and none of Customer's Affiliates, majority or minority owned subsidiaries, parent companies, or any other related entities, whether created through a divestiture or reorganization or acquired by purchase, merger, consolidation or otherwise, shall access or use Okta for AI Agents for Okta Customer Identity, including the OCI Agentic Identity Services, and such Okta Services shall not be used for the benefit of (e.g., to identify, authenticate, govern or manage) such entities or for any unrelated third party.
4.4.7 Licensing**.** Okta for AI Agents for Okta Customer Identity is licensed based on the number of Monthly Active Users per Year ("MAUs per Year"). For more information, see the Product Subscription Reference Guide.
4.4.8 Public Sector Exclusions. Okta for AI Agents for Okta Customer Identity in Okta for Government Moderate, Okta for Government High, or Okta for U.S. Military environments explicitly exclude any features that have not yet received a FedRAMP Moderate, FedRAMP High, or U.S. Department of Defense (DoD) Impact Level (IL) authorization. For a current list of excluded features, please refer to the Okta US Public Sector Limitations or Exceptions documentation at https://support.okta.com/help/s/article/okta-us-public-sector-limitations-or-exceptions?language=en_US, which Okta may update from time to time. For Customers deployed outside of these specified Public Sector environments, the purchase of Okta for AI Agents for Okta Customer Identity includes the standard features of the SKU, including features that do not yet have a FedRAMP or DoD IL authorization.
4.4.9 Subscription Renewal**.** Upon expiration of the current Term for Okta for AI Agents for Okta Customer Identity, the parties shall engage in commercially reasonable negotiations to renew the subscription. Customer acknowledges and agrees that such renewal shall be subject to Okta's then-current Units of Measure and pricing models at the time of renewal, which may vary from those set forth in this Order Form.

5. **Okta Digital Workers Service Specific Terms (last updated November 5, 2026).**

5.1 **Okta Digital Workers (last updated November 5, 2026).**

5.1.1 Applicability and Order of Precedence. These Service-Specific Terms apply solely to Customer's purchase and use of Okta Digital Workers.
5.1.2 Okta Digital Workers is a separate Service and SKU. It is not an AI Agent Service and is not subject to Section 2.1 of these Service-Specific Terms or any other Service-Specific Terms applicable to Okta for AI Agents, Auth0 for AI Agents, or another AI Agent Service.
5.1.3 These Service-Specific Terms supplement the Agreement. If there is a conflict between these Service-Specific Terms and the Agreement, these Service-Specific Terms control solely with respect to Okta Digital Workers.
5.2 Definitions. For purposes of these Service-Specific Terms:
5.2.1 "**Digital Worker Customer Resource**" or "**DWCR**" means any Customer or third-party system, application, account, network, database, infrastructure, service, software, data repository, or other resource that Customer connects to Okta Digital Workers or that Customer authorizes an Okta Digital Worker to access
5.2.2 "**Digital Worker**" means an AI-powered, purpose-specific software agent made available by Okta as part of Okta Digital Workers that performs configured tasks on Customer's behalf in connection with Digital Worker Customer Resources.
5.2.3 "**Outcome**" means a unit of measured consumption of Okta Digital Workers that is represented by one Verified Outcome.
5.2.4 "**Outcome Catalog**" means the applicable Order Form, Documentation, or other written description made available by Okta that identifies the Digital Workers, supported tasks, and applicable Verified Outcome types.
5.2.5 "**DW Subscription Term**" means the period during which Customer is authorized to use Okta Digital Workers, as stated in the applicable Order Form. The DW Subscription Term is part of the Term applicable to the Okta Digital Workers subscription under the Agreement.
5.2.6 "**Subscription Year**" means each consecutive twelve-month period beginning on the first day of the DW Subscription Term and each anniversary of that date during the DW Subscription Term. If the DW Subscription Term is less than twelve months, the entire DW Subscription Term is one Subscription Year. If the final period of a multi-year DW Subscription Term is less than twelve months, that final period is a Subscription Year
5.2.7 "**Verified Outcome**" means a new finding or independently completed job that: (i) is identified in the applicable Outcome Catalog; (ii) is completed by a Digital Worker in accordance with Customer's configuration and authorized permissions; and (iii) is supported by evidence recorded by Okta Digital Workers or otherwise made available by Okta.
5.2.8 "**Verified Outcome Credit**" means the contractual right to consume one Verified Outcome during the applicable Subscription Year. Verified Outcome Credits are not currency, stored value, prepaid funds, refunds, or credits toward another Okta product or service.

5.3 Scope of Use.

5.3.1 Okta Digital Workers allows Customer to configure and use Digital Workers to perform supported tasks on Customer's behalf in connection with Digital Worker Customer Resources (DWCR).

5.3.2 Customer may use Okta Digital Workers only for Customer's internal business purposes, in accordance with the Agreement, the applicable Order Form, these Service-Specific Terms, the Outcome Catalog, and Documentation.

5.3.3 Customer may connect only DWCRs for which Customer has all necessary rights, permissions, licenses, consents, and authority to authorize access and actions by Okta Digital Workers.

5.4 Verified Outcome Credits and Subscription Consumption.

5.4.1 The Product Subscription Reference Guide shall not apply to Okta Digital Workers. (i) Customer may consume up to the number of Verified Outcome Credits specified in the applicable Order Form during each Subscription Year. (ii) A specific Verified Outcome consumes one Verified Outcome Credit or (if greater) the number of Verified Credits indicated in the Outcome Catalog. (iii) Verified Outcome Credits apply only to the Subscription Year for which they are allocated. Any unused Verified Outcome Credits automatically expire at the end of the applicable Subscription Year. (iv) Unused Verified Outcome Credits do not carry over, roll over, transfer, or apply to a subsequent Subscription Year, renewal DW Subscription Term, other Order Form, other Okta service, or other Customer account. (v) Unused Verified Outcome Credits have no cash value, refund value, exchange value, or residual credit value. (vi) Except as expressly stated in the applicable Order Form, Customer may not reduce its annual Verified Outcome Credit allocation during the DW Subscription Term.

5.5 Outcome Measurement.

5.5.1 The following rules apply to Outcome measurement: (i) **Independent Access Removals**. Each verified independent access removal counts as one Outcome. (ii) **Inherited Permissions**. A single account or role change that removes multiple inherited permissions counts as one Outcome. (iii) **Issue and Fix**. A new verified issue and its subsequent verified fix together count as one Outcome. The same issue and fix will not count as more than one Outcome across Subscription Years unless there is a distinct and evidenced recurrence. (iv) **Onboarding Packages**. Each agreed application or Digital Worker onboarding package identified in the Outcome Catalog counts as one Outcome. (v) **Temporary Access**. A temporary access grant and its scheduled expiration together count as one Outcome. (vi) **Excluded Activities**. The following do not count as Outcomes and do not consume Verified Outcome Credits: technical steps; intermediate actions; raw alerts; system scans; duplicate findings; copies; retries; Digital Worker error repairs; false findings; unverified work; human-performed remediation; work completed by Customer or a third party; and observation or reporting of work already completed. (vii) **Reopened Issues**. A reopened unresolved issue does not consume an additional Verified Outcome Credit. A distinct and evidenced recurrence may qualify as a new Verified Outcome. (viii) **Outcome Records**. Okta's records of Verified Outcomes and Verified Outcome Credit consumption control for billing and consumption purposes, absent manifest error. Upon Customer's reasonable written request, Okta will provide reasonable information about a disputed Verified Outcome, subject to Okta's confidentiality, security, privacy, and legal obligations.

5.6 Excess Consumption and Upsell.

5.6.1 Outcome capacity is measured on a cumulative basis across each Subscription Year. In the event Customer exceeds, or is projected to exceed, its annual committed allocation of Verified Outcome Credits in any Subscription Year, Customer agrees to enter into an additional Order Form with Okta to increase its committed allocation to the next applicable tier of Verified Outcome Credits for each of the remaining Subscription Years through the expiration of the DW Subscription Term.

5.6.2 If Customer reaches its committed allocation prior to executing an upsell Order Form, Okta will notify Customer and the parties will work in good faith to promptly execute the required upsell Order Form. Continued sustained usage in excess of the committed allocation without an executed upsell Order Form following reasonable written notice may be treated as excess use under the terms of the Agreement.

5.7 Customer Configuration and Oversight.

5.7.1 Customer is solely responsible for the configuration and use of each Digital Worker, including: (i) the tasks, workflows, instructions, prompts, rules, triggers, and operating limits assigned to the Digital Worker; (ii) the DWCRs connected to the Digital Worker; (iii) the credentials, permissions, access scopes, tokens, approvals, and access controls granted to the Digital Worker; (iv) the data made available to the Digital Worker; (v) the human review, approval, monitoring, escalation, audit, rollback, backup, and recovery processes Customer uses in connection with the Digital Worker; and (vi) all actions taken by a Digital Worker in accordance with Customer's configuration, permissions, instructions, or authorized workflows.

5.7.2 Customer must review and test each Digital Worker's configuration before authorizing the Digital Worker to act in a production DWCR. Customer must use appropriate safeguards based on the nature and potential impact of the tasks the Digital Worker is authorized to perform, including least-privilege access controls, approval workflows, audit logging, backups, and recovery procedures.

5.8 DWCRs and Non-Okta Products.

5.8.1 Customer is solely responsible for DWCRs, including the availability, security, configuration, accuracy, integrity, functionality, content, and permissions of DWCRs.

5.8.2 Customer is responsible for its relationship with each provider of a DWCR, including a Non-Okta Product.

5.8.3 Okta does not control DWCRs or Non-Okta Products. Changes to DWCRs or Non-Okta Products, including changes to application programming interfaces, permissions, credentials, functionality, access controls, rate limits, terms, or availability, may affect the operation of Okta Digital Workers.

5.8.4 Customer must maintain appropriate backups, business continuity procedures, recovery procedures, audit logs, and access controls for DWCRs.

5.9 Actions in Customer Resources; Data Loss Disclaimer.

5.9.1 Digital Workers may take actions in DWCRs based on Customer's configuration, instructions, permissions, workflows, and connected applications. Such actions may include creating, changing, transmitting, revoking, disabling, deleting, or otherwise affecting data, records, accounts, access rights, permissions, configurations, or other DWCRs.
5.9.2 To the maximum extent permitted by applicable Law, and without prejudice to the limitations and exclusions of liability in the Agreement, Okta is not responsible for any loss, corruption, deletion, alteration, unavailability, disclosure, or damage to data or other content in a DWCR that results from: (i) Customer's configuration, instructions, permissions, credentials, prompts, workflows, or use of a Digital Worker; (ii) actions taken by a Digital Worker in accordance with Customer's configuration, instructions, permissions, credentials, prompts, or workflows; (iii) DWCRs or Non-Okta Products; (iv) Customer's failure to maintain appropriate access controls, approvals, monitoring, backups, audit logs, recovery procedures, or other safeguards; or (v) inaccurate, incomplete, unavailable, corrupted, or unauthorized data, instructions, permissions, or inputs made available by Customer or a third party.
5.9.3 Customer is responsible for promptly reviewing Digital Worker activity and taking corrective action if Customer identifies an incorrect, unintended, or unauthorized action. Customer is solely responsible for restoring or remediating DWCRs.
5.10 Customer Data and Sensitive Data.
5.10.1 Customer Data has the meaning given in the Agreement and includes electronic data submitted by or on behalf of Customer or its Users to the Service
5.10.2 Customer must not submit or make available any sensitive data to Okta Digital Workers, including without limitation, any personal health information, credit card data, personal financial data or other data that may impose on Okta specific data security, data protection or regulatory obligations in addition to, or different from, those specified in the Agreement, the DPA or the Documentation. The Agreement restricts Customer from sending or storing sensitive data in the Service unless otherwise set forth in an Order Form.
5.10.3 Customer is responsible for determining whether Customer Data or data in DWCRs is appropriate for use with Okta Digital Workers and for complying with applicable Laws, including (without limitation) privacy, data protection, employment, consumer protection, records retention, export control, and sector-specific requirements.
5.11 Restrictions.
5.11.1 Customer must not, and must not permit any User or third party to (i) configure or use a Digital Worker to access a DWCR without the necessary authorization; (ii) use Okta Digital Workers in violation of applicable Laws, third-party rights, the Agreement, these Service-Specific Terms, Documentation, or the applicable Order Form; (iii) use Okta Digital Workers to make a decision or take an action where applicable Law requires human review, consent, notice, or another safeguard that Customer has not implemented; (iv) circumvent, disable, interfere with, obscure, manipulate, or attempt to falsify any metering, reporting, monitoring, security control, Verified Outcome record, or Verified Outcome Credit calculation; (v) use Okta Digital Workers to introduce Malicious Code, gain unauthorized access to a system, disrupt or interfere with a system, or facilitate unlawful conduct; or (vi) use Okta Digital Workers in a manner that threatens the security, integrity, or availability of the Service, DWCRs, a Non-Okta Product, or another Okta customer.
5.12 No Professional Advice; Customer Decision-Making.
5.12.1 Okta Digital Workers may generate findings, recommendations, summaries, classifications, analyses, proposed actions, or other outputs. Customer is solely responsible for reviewing those outputs and determining whether, when, and how to act on them.
5.12.2 Okta Digital Workers do not provide legal, financial, tax, medical, employment, security, compliance, or other professional advice. Customer must obtain independent professional advice where appropriate.
5.13 Product Availability, Support, and Changes.
5.13.1 Notwithstanding anything to the contrary in the Agreement, Okta Digital Workers is a standalone platform that may depend on DWCRs, Non-Okta Products, third-party services, data sources, models, application programming interfaces, and integrations that are outside of Okta's control.
5.13.2 Okta does not warrant that Okta Digital Workers will be compatible with every DWCR or Non-Okta Product, operate without interruption, identify every issue, complete every requested task, produce error-free outputs, or prevent unintended actions in DWCRs.
5.13.3 Except as expressly stated in the applicable Order Form, Okta does not provide implementation, configuration, migration, workflow design, data remediation, monitoring, or managed services for Okta Digital Workers. The Agreement distinguishes Professional Services from the Service, and any implementation or configuration services should be separately described in a Statement of Work.
5.13.4 Okta may modify, update, suspend, limit, or discontinue a Digital Worker, a supported task, an integration, an Outcome type, or an Outcome Catalog item. Okta will notify Customer through changes to the Documentation or release notes for the Service. Okta will not materially reduce the core functionality of purchased Okta Digital Workers during the applicable DW Subscription Term except where required for security, legal compliance, platform integrity, or the discontinuation or material change of a DWCR, Non-Okta Product, third-party dependency, or underlying technology.
5.14 Excluded Environments and Uses.
5.14.1 Unless expressly stated in an applicable Order Form and supported by applicable Documentation, Okta Digital Workers is not authorized for: (i) classified environments; (ii) systems subject to U.S. Department of Defense Impact Level requirements; (iii) for United States federal government use; (iv) use cases that require FedRAMP authorization, StateRAMP authorization, or another government authorization not expressly identified by Okta as applicable to Okta Digital Workers; (v) use with protected health information, payment card data, government identifiers, Social Security numbers, or other sensitive or regulated data; or (vi) use in connection with a safety-critical system, including a system where a Digital Worker action could reasonably be expected to cause death, personal injury, physical damage, or material environmental harm.
5.15 Certifications, Authorizations, Security Documentation, and Data Protection Exclusions.

5.15.1 Notwithstanding anything to the contrary in the Agreement, any Order Form, the Documentation, the Data Processing Addendum, the Okta Privacy Policy (www.okta.com/legal/privacy-policy/), or the Okta Trust and Compliance Documentation, Okta Digital Workers is not included within the scope of any Okta certification, attestation, audit report, authorization, assessment, security standard, privacy standard, regulatory framework, or compliance program unless Okta expressly identifies Okta Digital Workers as in scope in writing.
5.15.2 Without limitation, Okta makes no representation, warranty, or commitment that Okta Digital Workers is or will be included within the scope of any SOC 1, SOC 2, SOC 3, ISO certification, FedRAMP authorization, StateRAMP authorization, HIPAA alignment, HITRUST certification, PCI DSS assessment, Department of Defense authorization, or other certification, attestation, authorization, audit, or compliance program.
5.15.3 The DPA applies to Okta Digital Workers only to the extent that Okta processes Personal Data (as defined in the DPA) submitted by Customer to Okta Digital Workers as Customer Data on Customer's behalf. Customer must not submit or make available sensitive data to Okta Digital Workers unless expressly permitted in an applicable Order Form. The Okta Privacy Policy does not expand the scope of Okta Digital Workers or create any product-specific representation, warranty, or compliance commitment for Okta Digital Workers.
5.15.4 Customer is solely responsible for determining whether its use of Okta Digital Workers, including its configuration of Digital Workers and connections to DWCRs and Non-Okta Products, is appropriate for Customer's privacy, security, compliance, regulatory, data residency, and data retention requirements.
5.16 Liability and exclusions.
5.16.1 WITHOUT PREJUDICE TO THE OTHER LIMITATIONS AND EXCLUSIONS OF LIABILITY IN THE AGREEMENT, OKTA'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO OKTA DIGITAL WORKERS SHALL NOT EXCEED THE TOTAL AMOUNT PAID AND PAYABLE BY CUSTOMER TO OKTA OR TO AN OKTA PARTNER FOR THE USE OF THE OKTA DIGITAL WORKER SERVICES GIVING RISE TO THE LIABILITY IN THE TWELVE (12)-MONTH PERIOD PRECEDING THE MOST RECENT INCIDENT OUT OF WHICH THE LIABILITY AROSE, (OR, FOR A CLAIM ARISING BEFORE THE FIRST ANNIVERSARY OF THE START DATE OF THE DW SUBSCRIPTION TERM, THE AMOUNT PAID OR PAYABLE FOR THE FIRST TWELVE (12)-MONTH PERIOD). THE FOREGOING LIMITATION SHALL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY.
5.16.2 OKTA SHALL HAVE NO LIABILITY OR OBLIGATION WITH RESPECT TO THE AVAILABILITY OF OKTA DIGITAL WORKERS AND ANY SERVICE LEVEL AGREEMENT FORMING PART OF THE AGREEMENT SHALL NOT APPLY TO OKTA DIGITAL WORKERS.
5.16.3 THE SECURITY MEASURES AND SAFEGUARDS SET OUT IN THE TRUST & COMPLIANCE DOCUMENTATION DO NOT APPLY TO OKTA DIGITAL WORKERS WHICH MAY EMPLOY LESSER OR DIFFERENT SECURITY MEASURES.
5.16.4 NOTWITHSTANDING ANYTHING TO THE CONTRARY SET FORTH HEREIN, THE FOREGOING EXCLUSIONS OF LIABILITY WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.