okta

OKTA, INC.
SERVICE-SPECIFIC TERMS

These Service-Specific Terms (the "SSTs") are between Okta and Customer. By executing an Order Form that references the SSTs or by otherwise accepting them, Customer agrees to the SSTs. Capitalized terms used in the SSTs not otherwise defined herein have the meanings given to them in the Agreement.

1.   General Terms.

1.1.   Okta may update or modify the SSTs from time to time.
1.2.   Updates or modifications to the SSTs will take effect (a) immediately, in the case of updates or modifications pertaining to new products or features or (b) upon renewal or execution of the applicable Order Form, for other updates or modifications.

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

2.1.   HRI Service is only offered as an add-on SKU for Enterprise Plans.
2.2.   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.   Client-Initiated Backchannel Authentication ("CIBA Service") (last updated September 15, 2025).

3.1.   The CIBA Service is included in all Auth0 Plans.
3.2.   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,
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, and
d)   CIBA includes second factor support for Auth0 Guardian, SMS, Email, and Voice (not available in Free Plans) and others as updated. SMS is charged separately by carriers supported by Auth0. Details are listed at https://auth0.com/docs/multifactor-authentication.

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

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

5.   Attack Protection Package (last updated August 15, 2025).

5.1.   Attack Protection Package is only offered as an add-on SKU for Enterprise Plans.
5.2.   Attack Protection Package enhances attack protection and security measures by enabling the Credential Guard, and Bot Detection functionality; additional usage details are listed at https://auth0.com/docs/attack-protection.