# EQUINIX SMARTKEY POLICY

This Equinix SmartKey Policy ("Policy") supplements other Equinix agreements and sets forth additional terms and conditions governing the use of Equinix SmartKey ("Service") by the Customer, as detailed in any applicable Order.

## 1. Definitions

Capitalized words used in this Policy will have the meaning ascribed to them herein, but if not defined in this Policy, shall have the meaning ascribed to them in the agreement governing the use of the Service.

**A. Key Operation** means an operation from one of the following key management and cryptographic operation categories performed through the Service, as further described in the Documentation: (1) authentication; (2) security objects; (3) encryption and decryption; (4) sign and verify; (5) digest; and (6) wrapping and unwrapping.

**B. Service Level Agreement** means the service level agreement set forth in Exhibit A of this Policy.

**C. Service Region** means the specific geographic territory from which the SmartKey Service is provisioned as identified in the applicable Order.

**D. Usage** means the number of Key Operations performed by Customer in connection with the use of the Service.

**E. Federal Information Processing Standard ("FIPS")** means a set of computer security standards developed by the National Institute of Standards that is used to certify cryptographic modules.

**2. Service Use Limitations.** In addition to the Service use limitations set forth in the Agreement, Customer agrees as follows:

1. Each Authorized User of the Service will be associated with a single, unique email address for purposes of accessing (and being identified within) the Service. Only Authorized Users may access or use the Service under Customer's account. Authorized User credentials cannot be shared or used by more than one individual.

2. Subject to Customer's compliance with the terms of this Policy and the Agreement, Equinix will provide Customer access to the Service as described herein and on the applicable Order. Equinix will provide Customer with Service on an as-is as-available basis unless the Parties agree to a Service Level Agreement. Customer's use of the Service is expressly limited to Usage and Service Regions for which Customer has paid the applicable Fees in accordance with the applicable Order.

3. The amount of Usage purchased may be modified during a given Term upon written agreement of the parties.

4. Customer understands that failure to protect security credentials may allow an unauthorized person or entity to access the Service. In addition, Customer acknowledges that Equinix does not have access to and cannot retrieve lost security credentials.

5. Customer shall not use the Service to store credit card information.

6. Customer is not permitted to resell the Service.

## 3. Non FIPS Mode

Unless otherwise agreed to in writing, the SmartKey Service is deployed in a non FIPS mode.

# EXHIBIT A

## SMARTKEY SERVICE LEVEL AGREEMENT

The purpose of this Service Level Agreement ("SLA") is to define the measurable performance levels of the Service licensed in accordance with the Digital Services Agreement or similar agreement entered into between Equinix and Customer ("Agreement") and specifies the remedies available to Customer if Equinix fails to achieve these levels. This SLA only applies to Customer's purchase of the Enterprise version of the Service, as designated in the applicable Order.

### 1. Definitions

All capitalized terms used in this SLA but not defined will have the meaning ascribed to the term in the Agreement or Equinix SmartKey Policy. The following additional definitions apply to this SLA.

- "**Downtime**" means a five-minute period during which at least ten Valid Requests are received and during which the Error Rate is 10% or more. For purposes of clarity, there is no Downtime if the Error Rate temporarily exceeds 10% during such five-minute period, provided that the aggregate Error Rate during a five-minute period does not exceed 10%.

- "**Error Rate**" means the percentage of total Valid Requests received in a period of time that result in a Response Error, excluding any Response Errors that are Excused Errors. Error Rate is determined by Equinix's server-side health monitoring. Expressed another way, Error Rate is calculated as follows.

$$\text{Error Rate} = \frac{\text{Number of Response Errors in a period} - \text{Number of Excused Errors in such period}}{\text{Number of Valid Requests in such period}} \times 100$$

- "**Excluded Operation**" means an operation from one of the following user, administrator and account management categories performed through the Service, as described in the published API documentation: (1) SmartKey authentication; (2) apps; (3) groups; (4) accounts; (5) users; (6) logs; and (7) plug ins.

- "**Excused Error**" means a Response Error that is due to: (a) circumstances beyond Equinix's reasonable control including without limitation, denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties, and other force majeure items; (b) Customer's act or omission, or the act or omission of any third- party partner with whom Customer connects; (c) any service failure of a third party system which Customer is using in conjunction with the Service, including but not limited to those provided by an Internet service provider, network service provider, or cloud service provider; (d) periods of scheduled or emergency maintenance activities or other scheduled periods during which the Service will not be available; (e) Customer-provided content, data or information or programming errors by Customer; (f) lack of availability by Customer or a failure of Customer to respond in a timely manner to incidents that require its participation for source identification and/or resolution, including meeting Customer responsibilities for any prerequisite services; or (g) Customer's breach of any of its material obligations under the Agreement.

- "**Included Operation**" means an operation from one of the following key management and cryptographic operation categories performed through the Service, as described in the published API documentation: (1) authentication; (2) security objects; (3) encryption and decryption; (4) sign and verify; (5) digest; and (6) wrapping and unwrapping.

- "**MRC Credit**" means a credit of a percentage of the monthly bill paid by Customer for the Service to be applied to future monthly payments by Customer for the Service that is offered due to a failure to meet the Monthly Uptime Objective, as further described in Section 3.

- "**Monthly Uptime Objective**" means 99.9%.

- "**Monthly Uptime Percentage**" means the percentage of time in a month that the Service is available, calculated as:

$$\text{Uptime Percentage} = \frac{\text{Total minutes in a month} - \text{Total minutes of Downtime}}{\text{Total minutes in a month}} \times 100$$

- "**Response Error**" means a response by the Service to a Valid Request within ten seconds of receipt of such Valid Request of HTTP Status 50x and with one of the following codes: (i) "Internal Error", (ii) "Unknown" or (iii) "Unavailable".

- "**Valid Request**" means a request issued by Customer to the Service to perform an Included Operation that conforms to the then-current Documentation, and that would normally result in a non-error response. For purposes of clarity, requests for Excluded Operations are not deemed Valid Requests and are not subject to this SLA.

## 2. MRC Credits

If the Monthly Uptime Percentage does not meet or exceed the Monthly Uptime Objective in any given month, Customer will be eligible to receive MRC Credits as specified below:

| Monthly Uptime Percentage | Minutes of Downtime (based on 30 day average) | MRC Credit |
|---|---|---|
| ≥ 95 to < 99.9% | 44 minutes to ≤ 36 hours | 10% |
| < 95% | > 36 hours | 25% |

The MRC Credits listed above are Customer's sole and exclusive remedy for any failure of the Service, including, without limitation, any failure to meet the Monthly Uptime Objective.

## 3. MRC Credit Requests

To receive an MRC Credit, as described above, Customer must notify Equinix Help Desk within five (5) days of any Downtime in any particular month and request a credit within thirty (30) days of the end of each month during which the Monthly Uptime Percentage failed to meet the Monthly Uptime Objective. All periods of Downtime must be verified by Equinix. Failure to comply with this requirement will result in waiver of Customer's right to receive an MRC Credit.

Approved credits will be applied by Equinix to Customer's invoice for the Service for the month following the month in which the MRC Credit was approved.