Biometric Information Security Policy for Illinois Contractors

1 Purpose and Objective

1.1 This Biometric Information Security Policy ("Policy") sets forth the policy and procedures of Digital Realty Trust, Inc. and its subsidiaries, and its affiliates (together, "Digital Realty") to the extent it may collect use, store, and/or destroy any biometric data for purposes of authenticating the access by Contractors to Digital Realty data centers, offices, and facilities and/or for timekeeping purposes in the state of Illinois in the United States.

2 Scope

2.1 This Policy applies to all business units, subsidiaries, and affiliate companies, worldwide, within Digital Realty, and sets forth the Biometric Information Security Policy pertaining to Digital Realty Contractors accessing Digital Realty data centers, offices, and facilities located in the state of Illinois in the United States.

3 Policy

3.1 As described herein, Contractor's biometric data may be collected for purposes of aiding Digital Realty in its business operations, including but not limited to authenticating Contractor's access to Digital Realty data centers, offices, and facilities and/or for timekeeping purposes.

3.2 A Contractor's biometric data will not be collected by Digital Realty or its authorized third-party vendors without the prior consent of the Contractor.

3.3 Digital Realty, through the provision of this Policy, will inform the Contractor of the reason his or her biometric data is being collected and the length of time the biometric data will be stored.

3.4 Digital Realty will not share the Contractor's biometric data with any third-parties unless otherwise disclosed in this Policy and without previously obtaining the Contractor's consent.

3.5 Any biometric data collected pursuant to this Policy will be destroyed within a reasonable period of time after the purpose for collecting the biometric data has been fulfilled, and in no event more than 24 hours after the collection of the biometric data as described below.

3.6 Procedures:

3.6.1 To ensure only authorized individuals have access to Digital Realty data centers, offices, and facilities, Digital Realty requires all visitors, including Contractors, to verify they have the appropriate permission to enter the data center, office, or facility by swiping a "smart card" ("Smart Card") that has been generated for them using authentication software provided by Digital Realty's authorized authentication vendor ("Vendor").

3.6.2 To generate these Smart Cards, a temporary scan of the Contractor's fingerprint is taken using a device and software provided by the Vendor.

3.6.3 During the fingerprint scan, the Vendor's device utilizes a proprietary algorithm to extract unique data (minutia) from the Contractor's fingerprint and thereby converts these data points into a binary code that is specific to the Contractor.

3.6.4 The binary code—and not the fingerprint—is stored in an encrypted state on the Smart Card using AES 256 encryption.

3.6.5 The temporary scan of the Contractor's fingerprint is immediately deleted and purged from the Vendor's device.

3.6.6 All authentication, storage, and matching of the encrypted binary code is completed via the Smart Card, and is not reliant on storage or authentication on any server or database.

3.6.7 No image or copy of the Contractor's fingerprint or fingerprint data is shared with or communicated to Digital Realty or the Vendor.

3.6.8 No image or copy of the Contractor's fingerprint is saved or stored on the Smart Card, on the Vendor's device, by the Vendor, or by Digital Realty, and the binary code stored on the Smart Card cannot be reverse-engineered to reproduce the Contractor's fingerprint.

3.6.9 The Smart Card, the Vendor's device, the Vendor, and Digital Realty do not create or save the type of image file required by the Integrated Automated Fingerprint Identification System, the national fingerprint and criminal history system maintained by the Federal Bureau of Investigation Criminal Justice Information Services Division, nor is the encrypted binary code stored on the Smart Card suitable for law enforcement fingerprint matching.

3.6.10 After Contractor's relationship or contract with Digital Realty is terminated, Digital Realty immediately deactivates the Smart Card. Thereafter, Contractor may relinquish its Smart Card, which is then securely destroyed within 7 days. If Contractor does not relinquish its Smart Card, Contractor (as the individual in possession of the Smart Card at the time of termination) is thereafter obligated to securely destroy the Smart Card.

3.7 The Effect of This Policy: This Policy is intended to supplement Digital's Privacy Practices (which can be found at https://www.digitalrealty.com/privacy), and supersedes all previous policies relating to the collection, use, storage, and destruction of biometric data by authorized third-parties for purposes of authenticating Contractor's access to Digital Realty data centers, offices, and facilities. To the extent there is any conflict between this Policy and Digital's Privacy Practices, this Policy shall control, but only as it relates to Digital's policies and practices relating to the collection, use, storage, and destruction of biometric data.

3.8 Updates to This Policy: In the event Digital Realty requires the collection of biometric data for any additional purpose, Digital Realty will update this Policy.

3.9 Publication & Availability of This Policy: A copy of this Policy is available at every applicable Digital Realty data center, office, and facility.

3.10 Review and Consent to this Policy: To gain access to Digital Realty data centers, offices and facilities, all Contractors must review this Policy and sign the attached Consent to Collection of Biometric Data.

4 Definitions

4.1 Biometric Data: Biometric data refers to any information, regardless of how it is captured, converted, stored, or shared, that is based on an individual's biometric identifiers, which include the individual's fingerprint, retina or iris scan, scan of hand, face geometry, or voiceprint.

5 Related Documents

5.1 Privacy Policy

6 Revision History

6.1 Initial version

7 Consent to Collection of Biometric Data

7.1 As set forth in Digital Realty's Biometric Information Security Policy, Digital Realty hereby provides notice to you of the following:

7.1.1 Your fingerprint will be temporarily scanned for purposes of authenticating your access to Digital Realty's data centers, offices, and facilities and/or for timekeeping purposes.

7.1.2 A temporary scan of your fingerprint will be taken by a device provided by Digital Realty's third-party authentication vendor ("Vendor").

7.1.3 During the fingerprint scan, the Vendor's device will use a proprietary algorithm to extract unique data (minutia) from your fingerprint and convert those data points into a binary code that is specific to you.

7.1.4 That binary code will be encrypted and stored on a Smart Card for use by you—and you alone—to authenticate your access to Digital Realty's data centers, offices, and facilities and/or for timekeeping purposes.

7.1.5 After conversion to the encrypted binary code, the temporary scan of your fingerprint is immediately deleted and purged from the Vendor's device.

7.1.6 No image or copy of your fingerprint or fingerprint data is shared with or communicated to Digital Realty or its Vendor.

7.1.7 No image or copy of your fingerprint is saved or stored on the Smart Card, on the Vendor's device, by the Vendor, or by Digital Realty, and the binary code stored on the Smart Card cannot be reverse-engineered to reproduce the your fingerprint.

7.1.8 Upon the termination of your contract or relationship with Digital Realty, Digital Realty will deactivate your Smart Card. You may then relinquish your Smart Card for secure destruction 7 days thereafter or you will be required to securely destroy the Smart Card in your possession.

By signing the below and/or by clicking the "Accept" button, you agree you have reviewed and understand the Digital Realty Biometric Information Security Policy and this Consent to Collection of Biometric Data form. You also consent to and authorize the collection of your biometric data as described above by Digital Realty and its authorized third-party authentication Vendor.

Printed Name: _____

Signature: _____

Date: _____