DIGITAL REALTY
Data Center Solutions

Supplier/Partner Cyber and Physical Security Guidelines

1. Summary

These Supplier/Partner Cyber and Physical Security Guidelines list the requirements that each Digital Realty's Supplier or Partner ("You") must follow when (a) accessing Digital Realty designated facilities, networks or information systems, (b) handling confidential or personally identifiable information furnished by Digital Realty (collectively, Digital Realty facilities, networks, information systems, and confidential or personally identifiable information furnished by Digital Realty are referred to in these guidelines as "Digital Realty Assets").

You are responsible for making sure that your personnel, including your contractors and suppliers, (collectively "Personnel") who have access to Digital Realty Assets comply with these requirements. All references to Personnel below means those Personnel who have access to Digital Realty Assets. Additional security compliance requirements may be specified for a particular Supplier or Partner based on the specific scope of activities.

2. Requirements

a. General

You must meet the following requirements before and throughout the period that You or any of your Personnel access any Digital Realty Assets.

b. Security Policies

You must implement and maintain a robust, comprehensive set of written information and physical security policies approved by your management and available for review by Digital Realty. Your information and physical security policies must be reviewed and updated at regular intervals to address changes in risk.

c. Organization

i. Roles and responsibilities of your employees, contractors and service providers must be documented.
ii. Segregation of duties must be in place to ensure that Personnel can perform only those functions necessary to fulfill their responsibilities.
iii. You must have, and make available upon request, an up to date organizational chart that documents your employees, managers, contractors and other personnel and their reporting hierarchy.

d. Human Resources

i. You must complete background screening, consistent with and subject to applicable laws, for your Personnel. The background check must be completed at least 5 business days before your Personnel first get any physical or logical access to Digital Realty Assets, and then again, every 2 years as long as your Personnel have such access. The background check will include criminal arrest/conviction, employment history, education verification, serious unpaid and current delinquent debt, collections or judgments for the immediately preceding 7 years. You will determine whether any information revealed during the background screening is reasonably related to your work for or with Digital Realty. You will certify that You have conducted pre-placement and periodic checks consistent with these requirements and determined that it is appropriate to have each assigned Personnel access Digital Realty Assets.

ii. You must ensure that your Personnel agree in writing to abide by your security requirements and organizational policies and these requirements.

iii. You must have a comprehensive security awareness program for all Personnel, including training upon hire and periodically thereafter on the applicable security policies, procedures and requirements. All Personnel who will be granted access to Digital Realty Assets must be trained regarding their requirements to adhere to Digital Realty policies, including these security guidelines

iv. You must have formal disciplinary processes, as well as a process to revoke access, for Personnel who violate your security policies or these requirements.

v. Upon reassignment or termination of employment, You will promptly remove access to Digital Realty Assets, and confirm the reassigned or terminated Personnel have not retained any confidential or personally identifiable information furnished by Digital Realty.

vi. All Personnel must acknowledge that they understand their obligations to adequately protect Digital Realty Assets, and that they have received, read, understood and agree to comply with all Digital Realty security requirements.

e. Asset Management & Passwords
   i. You must create and maintain a current inventory of all information systems used to access or process Digital Realty Assets.
   ii. Information classification labels should be applied in accordance with a documented information and data classification policy.
   iii. You must have written procedures and policies governing the life cycle of your information systems and their secure disposal.
   iv. Use of group or shared accounts is prohibited.
   v. Digital Realty must approve all your Personnel having access to Digital Realty Assets. You must not create user accounts with access to Digital Realty Assets without the express approval of Digital Realty.
   vi. Except for complex passwords of at least 15 characters recorded in a password vault that supports strong encryption, our Personnel must not write down or otherwise record Digital Realty passwords or authentication credentials.

f. Access Control
   i. Access to Digital Realty Assets must be granted on a least privilege, need-to-know basis. Your Personnel must be granted only the minimum privileges necessary to perform job responsibilities.
   ii. You must perform quarterly reviews to ensure that Your Personnel's access to Digital Realty Assets is appropriate and complies with Digital Realty's security requirements.
   iii. Administrative rights shall be documented and approved in a system of record.
   iv. You must have a decommissioning process that removes Personnel's logical and physical access and privileges within 30 minutes of reassignment or termination of employment
   v. Logs of user access shall exist containing all activities performed on an information system.
   vi. Remote access to your systems used to access Digital Realty Assets shall require multi factor authentication (MFA).
   vii. Your Personnel will use a Digital Realty-mandated MFA system when authenticating to Digital Realty Assets unless otherwise specified by Digital Realty.
   viii. You must restrict connection times for idle systems used to access Digital Realty Assets to no more than 15 minutes of inactivity.

g. Cryptography
   i. You must have documented policies governing the use of cryptographic methods.
   ii. Cryptographic keys must be stored in a secure, tamper resistant manner that logs all access and modifications to keys.
   iii. You must use only modern, strong, industry standard encryption and hashing algorithms.
   iv. Data-at-rest encryption shall be used wherever Digital Realty furnished information is stored.
   v. Digital Realty furnished information that is sent over public networks must be encrypted using modern, strong, industry standard encryption algorithms with strong keys.
   vi. You must not send Digital Realty passwords via email or other unencrypted means.

h. Physical and environmental security
   i. You must use physical security controls to prohibit unauthorized access into facilities where Digital Realty Assets are stored or accessed and track and record access, including by visitors. Access records must be maintained for at least 180 days.
   ii. Access into any non-public area of your facilities must contain a mechanism to identify and authorize access into the area. Access rights must be reviewed and updated regularly.
   iii. Areas where data/information is processed or stored must contain preventive controls, such as clean desk policies and laptop locks, to mitigate the risk of data compromise. All documents or other tangible items that store or access Digital Realty Assets must be secured when not in use by authorized Personnel.
   iv. You must have plans to minimize the risk of unauthorized external or internal threats to your facilities where Digital Realty Assets are stored or accessed
   v. You must not permit off-site removal of your systems that access or store Digital Realty Assets without Digital Realty's written consent.

i. Operational Security
    i. Your systems used to store or access Digital Realty Assets shall be deployed in a consistent manner from a golden or standard image that has been configured securely based on recommendations published by the Center for Information Security ("CIS") or similar industry best practices.
    ii. Your systems used to store or access Digital Realty Assets shall have only necessary software installed and should have only necessary services running.
    iii. Your systems used to store or access Digital Realty Assets must run antivirus software at all times. The antivirus software must be able to detect and quarantine common malicious software. The antivirus system must be configured to check for and automatically apply signatures and other vendor-supplied updates daily.
    iv. You must not use software that is no longer supported by the software vendor on any system used to store or access Digital Realty Assets.
    v. You must monitor your software and hardware vendors and reputable industry sources for information about vulnerabilities that could affect your system.
    vi. You must resolve security vulnerabilities in accordance with the following timelines as determined by vendor-supplied or otherwise recommended risk rating:
        (a) Critical risk vulnerabilities must be addressed within one week of discovery.
        (b) High risk vulnerabilities must be addressed within one month of discovery.
        (c) Medium risk vulnerabilities must be addressed within three months of discovery.
    vii. Your systems used to store or access Digital Realty Assets must be configured to check for and apply vendor-supplied updates at least daily.
    viii. Your systems used to store or access Digital Realty Assets must run host-based firewall software at all times. The firewall must be configured to allow only network traffic required to perform functions needed to fulfill contractual commitments between Digital Realty and You.
    ix. Changes to your systems must be documented and approved by your designated personnel. Change management records must be stored in a system of record.
    x. You must conduct vulnerability assessments must be conducted at regular intervals to identify areas of weakness along with appropriate mitigation strategies.
    xi. Procedures should be in place to detect and recover from planned and unplanned service outages.
    xii. Your systems must create logs that record date, time and source (IP address/host), and the logs must be retained for at least 180 days.
    xiii. Digital Realty will, to the extent permitted by law, monitor your Personnel's access to and use of Digital Realty Assets.
j. Communications Security
    i. Policies governing the sharing of information should be in place.
    ii. Your networks should be designed for tiering or segmentation that limits an individual's ability to send network traffic to systems which are unrelated to the individual's job function.
    iii. You must create and maintain updated network architecture diagrams to reflect your current network topology.
k. System Acquisition, Development and Maintenance
    i. Modifications to applications or systems shall be logged and documented
    ii. You must employ a secure System Development Life Cycle when building software or systems that will be used in conjunction with Digital Realty data or systems.
l. Vendor Management
    i. Agreements shall be in-place to facilitate the modification of services rendered.
    ii. Vendors and partners used by You must follow documented security guidance.
m. Incident Management
    i. A Security Incident is any suspected or confirmed violation of Digital Realty's Cyber and Physical Security policies. This includes, but is not limited to, unauthorized access and attempts to gain unauthorized access to Digital Realty's systems, accidental disclosure of Digital Realty furnished confidential information and incorrect functioning of Digital Realty security controls (such as authentication systems).
    ii. All Security Incidents must be reported to Digital Realty immediately.
    iii. An incident response plan shall exist containing roles, responsibilities, notification lists, and processes to identify, mitigate, and contain information security incidents.
    iv. Regular testing of the incident response plan shall take place to gauge effectiveness and areas of improvement for the plan.

n. Business Continuity
    i. Business Continuity Planning ("BCP") policies, procedures, and standards shall exist that support agreed upon uptime levels.
    ii. Testing of BCP should take place on a scheduled basis with results recorded and documented in a system of record.
o. Compliance
    i. Applicable legal, regulatory, and contractual requirements must be defined and documented in a system of record.
    ii. Auditing of compliance adherence shall be documented and conducted on a scheduled basis.
    iii. Data owners and custodians shall be identified as responsible parties for the compliance of their data and systems.
    iv. If You access or process personal information, You will comply with any additional data processing requirements identified by Digital Realty.
    v. You will provide information and respond to questions about your security practices as may be requested by Digital Realty from time to time.
    vi. Digital Realty may perform security assessments.
    vii. You will promptly correct any identified noncompliance with your own security policies or Digital Realty security requirement identified by You or Digital Realty.
p. Risk
    i. You must engage with both inside and outside parties to perform risk assessments against both internal and public facing assets consisting of:
        (a) Penetration Tests
        (b) Web Application Security Assessments
        (c) Vulnerability Assessments
    ii. Known risks shall have the following documented:
        (a) Risk owner
        (b) Corrective action plan or risk acceptance form
    iii. You must apprise Digital Realty of any known security issues, prior breaches, or active compromise pertaining to information systems before and after access to networks, data or systems is provisioned.
q. Certifications
    i. You must maintain the certifications agreed to with Digital Realty, and provide written evidence, including the applicable Report on Compliance (ROC), if requested by Digital Realty.
    ii. If any material findings are noted by the third-party assessor, You will immediately notify Digital Realty and implement remediation pursuant to an agreed upon plan.