DIGITAL AND TECHNOLOGY

POLICY 5.5 INFORMATION ASSET PROTECTION

EFFECTIVE DATE: JUNE 1, 2000

REVISED: JUNE 1, 2000, October 2, 2007; November 2, 2012; July 16, 2013; November 30, 2016

I. INTRODUCTION

CBRE, Inc., ("CBRE" or Company") shall take appropriate and reasonable measures to safeguard the confidentiality, integrity, and availability of CBRE electronic networks, equipment, and information contained thereon.

II. APPLICABILITY

A. As appropriate:

1. This policy is applicable to all employees, independent contractors and consultants of the Company globally, and every person using electronic equipment or networks to conduct CBRE business regardless of whether such equipment or networks are owned by CBRE, or connected to CBRE systems.

2. This policy is applicable to all CBRE lines and departments globally, including all corporate office locations, lines of business, shared services and operational business units. It applies to independently operated subsidiaries such as CBRE Global Investors and Trammell Crow Company. The policy represents the minimum standards for Digital and Technology Disaster Recovery within the CBRE group.

III. DEFINITIONS

A. "Device" includes desktop computers, laptops, notebooks, hard or flash storage drives (or any other similar device), smart phones (Android, Apple, Blackberry, and Windows),or any other similar tablet/slate, PDA, phone or media device used to access Company Networks or Information Assets.

B. "Cloud Service Solutions" include all vendors and partners that provide usage-based services and the physical elements are not procured, stored, hosted or maintained by CBRE.

C. "Information Assets" includes:

1. Data, documents, data compilations, software or hardware stored, filed, created, documented and/or maintained, on or in connection with the Company's central computer network, systems or Cloud Service Solutions.

   a. CBRE's computer network or systems include but are not limited to the Lan and Wan Networks, Server Systems, Data Centers and all CBRE controlled systems.

2. Any Device (whether owned by CBRE or not) with access to or operating on CBRE Networks.

D. "Confidential Information" means Information Assets, which because of their sensitive nature should be treated confidentially due to the risk that unauthorized use, disclosure, destruction or modification could cause financial, reputational or other harm to the Company, employees, vendors or clients, or subject the Company to civil, criminal, regulatory or other legal sanctions. Confidential Information includes but is not limited to:

1. Personnel, medical, salary, performance or other employee records

2. Financial records, trade secrets, information subject to a confidentiality agreement,

3. Information deemed private or confidential by law,

4. Information deemed private or confidential by CBRE or Company vendors or clients.

5. Information which in the normal course of business is reasonably expected to remain confidential by CBRE employees, clients, vendors, regulatory bodies, and others, or any other.

E. Digital and Technology Disaster Recovery: Technology strategies and plans used to restore information assets, following a disruption to meet business and regulatory requirements.

F. Business Application Owner: An individual within the business team (as opposed to the Digital and Technology group or the Business Continuity Office) that is assigned ownership of an application or applications used by the business that will serve as a point of contact for Digital and Technology and the Business Continuity Office and will fulfill certain responsibilities within this policy.

IV. POLICY

A. Digital and Technology Activated Security Requirements

1. Certification

Individuals who use CBRE Networks or any Device for transacting CBRE business must certify annually that they have reviewed and are in compliance with this policy;

2. Passwords

a. The Company shall establish and maintain individual access identification and authentication security protocols for all relevant Networks and Devices that provide access to Information Assets. These protocols shall include but not be limited to the following minimum standards:

i. They shall be reviewed and assessed periodically to conform to regulatory changes or industry norms related to applicable Networks or Devices.

ii. Each individual accessing CBRE Networks must be assigned an individual access identification (“Password”).

iii. Security protocols must include Password expiration within a reasonable period, or upon termination of an employee or other person with access to Company Networks.

b. Password Assignments and Approvals.

i. The supervisor of an employee requiring access to Company Networks must approve and submit a Computer User Registration form to the appropriate person in Digital and Technology or HR. The Digital and Technology Service Desk (Service Desk) will then be instructed to provide the employee with access to the required Networks. This access will be based on the least required principle.

ii. Access by clients and/or other third parties, must be approved by the appropriate Department Manager and, where required, the Business Application Owner following the same procedures in the paragraph above.

c. Passwords Deemed Confidential.

i. CBRE deems Company required passwords to be Confidential Information.

Employees are prohibited from sharing a Password with any other person unless prior written authorization is obtained by the applicable Line of Business President, Senior Department leader, Regional Compliance Officer, or the General Counsel of the Company.

ii. Written authorization will only be granted in the rare circumstances when conditions prevent delegated access to be provided.

iii. Written authorization must be stored in the requesting employee's employment file maintained by HR.

d. Password Deactivation; Security Lockdown

i. When an employee or other person no longer requires access to Company Networks (e.g., leaves the Company, leave-of-absence, etc.), the appropriate supervisor or Department Manager shall immediately notify the HR or Legal Department so access privileges can be revoked.

ii. If access should need to be suspended due to a security risk, etc, the direct supervisor of the departing employee should contact the Digital and Technology Service Desk in addition to the steps above.

3. Screen lock

a. Technology permitting, Digital and Technology shall install and maintain a time activated automatic lockdown function ("Screen Lock") on all Devices with access to Company Networks. The purpose of the Screen Lock is to reduce the risk of unauthorized access to Networks and Information Assets should a Device be lost, misplaced, left unattended, or stolen.

b. The Screen Lock will activate upon a reasonable period of non-use of the Device, as determined by the Senior Manager of Digital and Technology or General Counsel, in consultation with senior business leaders. Once activated the Screen Lock will lock out access to the Device until the user inputs the correct Password. From time-to-time Digital and Technology will establish and communicate appropriate security protocols to address excessive attempts by a person to enter an incorrect Password.

4. Physical Security of Certain Information Assets

Digital and Technology will establish security standards for locations and facilities that store, process or maintain Digital and Technology Systems and Networks

5. Additional requirements for Smart Phones, Tablets, and Slate Devices.

a. In order to connect these types of Devices whether personally owned or CBRE owned, to CBRE systems or data the following additional requirements must be met.

i. Support remote wipe capability.

ii. Support over the air (OTA) configuration by CBRE including, password reset, device configuration, remote locking, and application installation/removal

iii. Digital and Technology will install management agents and/or configurations when connected to CBRE systems or data as appropriate.

iv. May not be jail-broken, rooted, or similar state where the underlying Operating System or bios has been compromised.

v. Running a CBRE supported operating systems or bios.

vi. Support encryption of data transmission and storage.

b. Before disposing or transferring ownership of a mobile device all CBRE data must be removed. CBRE may require a full or partial device wipe at its discretion.

c. CBRE will enforce full device wipe after a set number of failed login/unlock attempts.

d. Non CBRE owned or controlled data. This data may be wiped, erased, or otherwise accessed by CBRE in the course of securing or managing the Device.

e. If the Device is CBRE owned, only CBRE approved applications may be installed on it. CBRE IT will implement controls to enforce this requirement.

i. All accessories and software purchases for CBRE owned Devices must be pre-approved and adhere to CBRE enterprise standards, in compliance with CBRE's Travel and Expense Management Policy. The referenced T&E policy (Section 22.0- Non-Reimbursable Expenses) states that employees may not use their corporate credit card for such purchases.

f. These Devices may be subject to legal holds or discovery.

g. Location Services may be used with appropriate oversight to locate the device.

h. Digital and Technology will establish documented processes and controls enforcing these requirements.

B. Employee Security Requirements

1. Anyone with access to CBRE Information Assets, Networks, or Devices is expected to take reasonable measures to safeguard and protect them against unauthorized access, including but not limited to the following:

a. Mobile devices (laptops, smartphones, tablets/slates, PDAs, etc.) should be physically secured at the end of each workday removing them or locking them in a secure place (file cabinet, drawer, etc.).

b. While traveling personal possession of Devices should be maintained at all times unless prohibited by law or the transport company.

c. In accord with Section IV.A.2.c above, sharing of Network or Device Passwords or other personal user identification is prohibited.

d. The Screen Lock function on all Devices should be activated when left unattended during regular working hours and at the close of business. Unauthorized access or use of Confidential Information, or a lost or stolen Device, Password or Information Asset, should be reported immediately.

f. Only use CBRE authorized Cloud Service Solutions which meet CBRE security requirements.

C. Other Technical Security Requirements

Local computer administration rights will not be granted to CBRE new hires and to newly issued or reimaged/reissued CBRE-owned desktop and laptop computers. Exceptions may be granted based on the user's role or technical requirement as appropriate.

D. Confidential Information Assets

1. Reproduction or Distribution

a. Confidential Information may only be reproduced or distributed with prior authorization in accord with applicable policy, agreements, laws, or regulations.

b. Notwithstanding the above, reproduction or distribution of private or personal information such as employment records, health records, etc., requires approval of the General

Counsel, or the senior leader of the HR department.

2. Encryption of Confidential Information

a. Digital and Technology will develop and adopt encryption standards and protocols for the handling and transfer of Confidential Information in compliance with the minimum requirements of the most stringent applicable laws or regulations.

3. Disposal of Confidential Information

a. Disposal of Confidential Information may be accomplished through the shredding of paper media, raiser of magnetic data, or by delivery to a bonded salvage company, which will provide a written Certificate of Destruction or comparable document. Disposal of customer or vendor information may have specific requirements due to contractual agreements. Ensure that customer or vendor information is disposed according to those agreements.

E. Software Copyright and Intellectual Property

1. Third-party Software and Intellectual Property

a. CBRE prohibits illegal, unauthorized or unlicensed use of third-party software or other intellectual property on any Company Networks, or Devices used for CBRE work activities.

2. CBRE Proprietary Software and Intellectual Property

   a. All Information Assets developed by, for, or on behalf of CBRE by any Company employee(s), contractor(s), vendor(s), or any other source is:

      i. Owned by, and intended for the exclusive use of CBRE, and

      ii. May not be used for any other purpose unless expressly approved in writing by the Senior Manager of the Digital and Technology department and the Company General Counsel.

F. Security Awareness Training

1. An annual awareness training program for United States employees will be implemented by Digital and Technology. The program will cover issues in this policy including security, confidentiality and privacy. The program will be mandatory in states where required by law.

2. Each global region will adopt similar training programs if required by law.

G. Audits and Global Standards

1. Security controls will meet the minimum requirements of the most stringent laws or regulations globally or at the federal or state level, as relevant.

   a. On an annual basis Digital and Technology will audit the effectiveness of this and other Digital and Technology security, acceptable use, and confidentiality policies and related measures designed to protect Information Assets and Confidential Information.

   b. Digital and Technology will issue or update Global Required Minimum Security Standards based on the annual
   assessment described in the paragraph above. The Standards can contain non-material differences depending laws and local conditions in the various global regions in which CBRE maintains operations.

H. Digital and Technology Disaster Recovery Requirements

1. Roles and Responsibilities

   a. Business Continuity Office. The Business Continuity Office, with assistance from Digital and Technology and the business, is responsible for ensuring that Business requirements for IT resiliency are known and documented; The BCO is responsible for ensuring that significant risks
   associated with Digital and Technology recovery are managed and transparent.

   b. Digital and Technology Department: The Digital and Technology Department is responsible for:

      i. Creating, maintaining and testing Digital and Technology Disaster Recovery plans, and providing regular information on recovery risks and Digital and Technology Disaster Recovery status.

      ii. Maintaining a central database of information assets which includes business owners.

c. Business Applications Owners.

i. Responsible for communicating business requirements to Digital and Technology and the Business Continuity Office, and ensuring business support to complete Digital and Technology DR planning and testing, or acknowledging acceptance of risk.

ii. Responsible for notifying Digital and Technology and the Business Continuity Office when an application is no longer in use or the usage profile will substantially change. e.g. The amount of revenue generated will substantially increase, or the user base will substantially increase.

2. Requirements

a. The Digital and Technology Department and the Business Continuity Office will jointly develop standards to meet business and regulatory requirements for Digital and Technology Disaster Recovery. The standards will be updated or reviewed on an annual basis. The standards will define the operational procedures to ensure that:

i. On a regular basis, the Business Continuity Office department will request an assessment of the impact of a failure or outage for Information Assets from Business Application Owners.

ii. Digital and Technology Department will develop and maintain plans and procedures to ensure recovery capabilities meet business and regulatory requirements as defined by Business Owners.

iii. The Digital and Technology Department will ensure that recovery risks and Digital and Technology DR status of designated information assets are reported to Business Continuity Office on a regular basis.

iv. The Business Continuity Office will assess recovery risks. Significant risks require tracking and Business Application Owner notification. Where no resolution is intended, an acceptance of the risk must be acknowledged by the Business Application Owner.

I. Condition of Employment

1. Compliance with this policy is a condition of employment and/or continued affiliation with CBRE. Any person or entity who violates the policy, or attempts to subvert Company security, access controls, and/or other restrictions placed on the use of Networks or Devices shall be subject to discipline, up to and including termination.