Policy No. 14

Information Technology Use

TABLE OF CONTENTS

Purpose ............................................................................................................................. 2
Scope ............................................................................................................................... 2
I. Statement of Policy .................................................................................................... 2
A. JLL Property ............................................................................................................. 2
B. Privacy and Monitoring ......................................................................................... 2
C. Prohibited Activities ............................................................................................... 3
D. Software .................................................................................................................. 4
E. Copyright Issues .................................................................................................... 4
II. Best Practices Regarding Email, Voicemail, Internet Use, Computer Use, Personally-owned devices, Data Integrity, Anti-Virus Protection and Social Media ................................................................. 5
A. Security Awareness ............................................................................................... 5
B. Use of Email, Voicemail and Instant Messaging ...................................................... 5
C. Email Retention and Maintenance ....................................................................... 6
D. Internet Use ............................................................................................................ 7
   1. Acceptable Uses of the Internet ........................................................................... 7
   2. Unacceptable Uses of the Internet ...................................................................... 8
   3. Internet Communications ................................................................................... 8
E. Technology Use ....................................................................................................... 9
F. Personally Owned Devices ..................................................................................... 10
JLL Responsibility ....................................................................................................... 10
Employee/User Responsibility ....................................................................................... 11
G. Data Integrity .......................................................................................................... 12
H. Anti-Virus Protection .............................................................................................. 12
I. Social Media Guidelines ......................................................................................... 13
III. Miscellaneous Provisions ..................................................................................... 13
Policy Violations .......................................................................................................... 13
Related Global Policies ............................................................................................... 13
Administration of Policy .............................................................................................. 14
Legal Restrictions on the Application of this Policy in Particular Countries .............. 14
Restriction on Posting Company Policies .................................................................... 14
Revision History .......................................................................................................... 15

Policy No. 14
Page No. 1 of 16
Subject Information Technology Use
Issued By Global General Counsel
Revision Date 05/17/17
Purpose
Jones Lang LaSalle Incorporated (including its majority-owned subsidiaries, “JLL,” or the "Company") provides voicemail, email, instant messaging, Internet and network access, mobile devices and computer systems with associated software (“Information Technology Systems”) to assist Employees (as defined below) in the conduct of business for the Company.

Information Technology Systems are provided to Employees for the benefit of JLL and the work it does for its clients. Every Employee has a responsibility to maintain and enhance JLL’s public image, and to use the Information Technology Systems in a productive, environmentally responsible, and appropriate manner.

Scope
Compliance with this Policy and procedures is mandatory for all employees, as well as temporary employees, consultants, contractors, sub-contractors and anyone else who has access to Information Technology Systems (“Employees”).

I. Statement of Policy

A. JLL Property

The Information Technology Systems and the data/documents stored on them are and remain at all times JLL property. All business processes and software remain the intellectual property of JLL.

B. Privacy and Monitoring

1. Except as provided by applicable local laws, Employees have no right to privacy as to any information transmitted through or stored on the Company’s Information Technology Systems or other technology resources. JLL has access to all information on all Company Information Technology Systems. Notwithstanding the above, JLL will comply with all laws regarding the privacy of legally protected confidential information.

2. As a condition of use of the Information Technology Systems, Employees acknowledge and agree that JLL may, at its discretion and for legitimate business purposes, inspect, use, or disclose communications and related information without further notice. No personal privacy is assured with the use of the Information Technology Systems.

3. Our Information Technology Systems enable us to monitor, access, filter retrieve and / or read email, voicemail, instant messages, files and other communications composed, sent, reviewed or received, to safeguard the Company against irresponsible use. For business reasons, and in order to carry out legal obligations in our role as an employer,
your use of the Information Technology Systems (including any personal use) may be continually monitored by automated software or otherwise.

4. JLL reserves the right to retrieve the contents of email messages or check Internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including, but not limited to, the following:
   a. to monitor whether the use of the email system or the Internet is legitimate and in accordance with this Policy;
   b. to find lost messages or to retrieve messages lost due to computer failure;
   c. to assist in the investigation of alleged wrongdoing; or
   d. to comply with any legal obligation.

5. JLL has the authority to delete any non-business or non-employment related material without prior notification in accordance with applicable local laws.

6. Except as provided by applicable local laws, all communications including text and images may be disclosed to law enforcement or other third parties for legitimate business and / or legal purposes without prior consent of the sender or the receiver.

C. Prohibited Activities

1. Users are prohibited from sharing user-ids and passwords except when required to be disclosed to JLL Information Technology (i) as part of user requested trouble shooting, or (ii) required software installations. When a user-id or password is provided to JLL Information Technology it should be changed immediately after the trouble shooting or software installation is complete. User-ids must uniquely identify a single user.

2. Harassment of any kind is prohibited. Voice or electronic transmissions may not contain content that may reasonably be considered offensive or disruptive to any Employee. No messages may be transmitted with derogatory or inflammatory remarks about an individual or group’s gender, age, race, religion, national origin, physical attributes or sexual preference.

3. Storing, transmitting, downloading, processing, accessing, or displaying material that is offensive, hateful, obscene, vulgar, sexually explicit, or in violation of international, national or state regulation or law, or by the common law, is expressly forbidden.

4. Information Technology Systems must never be used to solicit for non-job-related commercial ventures, religious or political causes, or any other cause not related to the business of JLL.

5. Falsifying information of any kind regarding the business, the firm or yourself is illegal.

6. Employees are explicitly prohibited from sending unsolicited email messages from corporate email accounts (e.g. "junk mail" or "Spam").
7. Employees may not forward or otherwise propagate chain letters, whether or not the recipient wishes to receive such mailings.

8. Employees may not exchange non-public information related to the business of the firm over Information Technology Systems, cloud services, or other online data exchange services that have not been approved by JLL Information Technology (e.g. GoogleDocs, DropBox).

9. Personal web sites, applications or mobile applications (“Personal Online Content”) for personal use may not be established/set up using Information Technology Systems. Personal Online Content created for JLL business must be set up in accordance with JLL Information Technology procedures. JLL computers are strictly for business use only; JLL Information Technology will approve all sites hosted by the firm to ensure that they meet JLL standards.

10. Employees are prohibited from unauthorized access, review, duplication, dissemination, removal, damage or alteration of the following: files, passwords, computer systems, programs, voicemail messages or other Company property.

11. It is illegal for any Employee to commit forgery, including falsifying of any email information including headers, addresses, signatures, etc.

D. Software

1. Only Company approved software may be loaded on Company computers by JLL Information Technology.

2. A valid software license is required for each software package running on every computer. Using an unlicensed version of software constitutes a breach of the software supplier’s copyright.

3. Employees should not load software from any source on to a JLL computer that has not been authorized by JLL Information Technology. Note: in the event an Employee device must be restored, the device will be restored to standard build specifications, and only JLL provided software would be restored. Employee loaded personal software, is not the responsibility of JLL, and will not be supported or restored.

4. JLL Information Technology reserves the right to remove non-standard software from user computers when it is determined that the software poses a risk to normal business operations.

E. Copyright Issues

1. Users are not permitted to copy, transfer, rename, add or delete information or programs belonging to other users unless given express permission to do so by the owner.
II. Best Practices Regarding Email, Voicemail, Internet Use, Computer Use, Personally-owned devices, Data Integrity, Anti-Virus Protection and Social Media

A. Security Awareness

Employees are expected to understand common threats and user best practices associated with the use of Information Technology Systems. Security awareness is strongly encouraged and based on a risk assessment by individual business units to determine if it should be mandatory for that particular business unit. Training shall consist of relevant curriculum and an assessment designed to demonstrate understanding of key topics and concepts. Training opportunities shall be updated annually to reflect changes to the Company, to technology, and to the information security industry in general.

B. Use of Email, Voicemail and Instant Messaging

1. Reliability of passwords for maintaining email or voicemail confidentiality cannot be guaranteed. Users should assume that someone, other than the intended recipient, might read or listen to any and all messages. Avoid messages that contain information that should not be conveyed in public and remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

2. Employees may access only messages, files or programs that they have permission to access.

3. Instant Messaging may only be used to conduct Company business or to gain technical or analytical advice.
   a. All policies that govern the acceptable use of email also apply to Instant Messaging.
   b. Instant Messaging applications should be used for communicating non-sensitive business information only.
   c. Users should not rely on Instant Messaging applications to transfer and download files.

4. Deleting an email or voicemail message may not ensure instant removal from network resources. Please contact the Technology Service Desk for assistance in completely removing sensitive information.

5. Employees should not use personal email to conduct JLL business for any reason and shall not forward sensitive, confidential or proprietary email from their JLL email.
Corporate Governance and Compliance Policy Manual

Policy No. 14

Information Technology Use

account to a personal email account except, in limited circumstances, for a legitimate business purpose. For business purposes, it is recommended to use enterprise bulk mail services for marketing and promotional email.

6. Email and Internet use is covered by laws concerning storage and transmission of obscene or hateful literature. Usage may be monitored and any misuse by staff will not be tolerated. Violations of the law will be reported to the appropriate officials and the Company reserves the right to take disciplinary action where personal use of the Information Technology Systems is unreasonable, detrimental to the user’s job responsibilities, risks compromising the Company’s reputation and business interests, or exposes the Company to prosecution for illegal activities.

Note: Humor is a very personal thing and not everyone finds the same things funny. Please be aware that what you think is funny may be deeply offensive to the next person. Do not transmit messages containing sexual innuendoes, humor based on alleged stereotypes, or any other potentially offensive content.

7. Communications should clearly identify the originator and recipient. If you receive a communication by mistake, stop reading as soon as you realize it was not meant for you and notify the sender or the Technology Service Desk. It is not permissible to purposely read communications intended for another person without his or her permission. If you forward a communication originated by someone else, do not make changes without clearly stating that you have done so.

8. Outgoing email should contain the following disclaimer language at the bottom. This language is added by the Company email system by default, and should not be removed or altered:

This email is for the use of the intended recipient(s) only. If you have received this email in error, please notify the sender immediately and then delete it. If you are not the intended recipient, you must not keep, use, disclose, copy or distribute this email without the author's prior permission. We have taken precautions to minimize the risk of transmitting software viruses, but we advise you to carry out your own virus checks on any attachment to this message. We cannot accept liability for any loss or damage caused by software viruses. The information contained in this communication may be confidential and may be subject to the attorney-client privilege. If you are the intended recipient and you do not wish to receive similar electronic messages from us in future then please respond to the sender to this effect.

C. Email Retention and Maintenance

1. The Company’s Records Retention Policy mandates the retention of business records for the statutory retention period for each type of record. Electronic communications may be Company Records as defined in the Records Retention Policy found in the Corporate Governance and Compliance Policy Manual as Policy #10. Pursuant to this Policy, all electronic communications that are not to be saved as business records
Information Technology Use

should be deleted. Each user of email is responsible for determining which electronic communications should be retained as business records in accordance with the Records Retention Policy and their business unit’s retention requirements.

2. All electronic communications that must be retained are to be filed and retained in compliance with the specified retention period for the type of record. The filing requirement may be satisfied by either filing an electronic copy in an accessible mailbox or non-private electronic folder on the email system or Company network, or by printing and filing a hardcopy of the electronic communication and then deleting the communication from the email system. Automatic archiving or rule functions should not be used universally to save such records.

3. All electronic files kept on the Information Technology Systems, or even maintained on other storage devices are subject to compulsory disclosure by subpoena or other lawful order of government officer(s), or discovery proceedings in a lawsuit. Failure to disclose or produce such electronic files or the alteration or deletion of electronic files that are identified by a court or federal agency for involuntary disclosure may subject the Employee and the Company to civil and/or criminal penalties.

4. As is more fully explained in the Records Retention Policy, all electronic files, including email items which relate in any way to the subject of ongoing or impending litigation or governmental investigation (including relating to the litigation or investigation itself) are to be maintained in a secure location until conclusion of the relevant dispute, as confirmed by Global Legal Services.

5. Personal and mailbox folders should be reviewed periodically to determine if continued retention of content is warranted. Automatic archiving or rule functions should not be used universally to save messages. It is the user’s responsibility to identify items that must be saved because of related ongoing or impending litigation, governmental investigation or other legal or personal requirements.

D. Internet Use

1. Acceptable Uses of the Internet

   Employees represent JLL when accessing the Internet using Company provided technology. Consequently:

   a. All Internet use should be for business reasons. JLL does permit limited personal use of the Internet and electronic mail facilities on the condition that Employees act sensibly and responsibly. The Company reserves the right to take disciplinary action where personal use of the Internet is unreasonable, detrimental to the user’s job responsibilities, risks compromising the Company’s reputation and business interests, or exposes the Company to prosecution for illegal activities.
b. Company Employees may not use the Internet to make disparaging comments about the Company or to disclose information about the Company other than in compliance with the Company's media and disclosure policies.

c. Internet databases may be accessed for research and information as needed.

e. Corporate email should be used for business contacts.

2. Unacceptable Uses of the Internet

Company provided Information Technology Systems should not be used to access the Internet:

a. to send, save or view offensive material;
b. to harass or discriminate;
c. for personal gain or advancement of individual views;
d. to solicit non-Company business; or
e. where such use disrupts the operation of JLL’s network or interferes with an Employee’s productivity.

3. Internet Communications

Employees shall use the Internet and JLL email in an ethical and lawful manner. Therefore:

a. Each Employee is responsible for the content of all text, audio or images that he or she places or sends over the Internet (including on personal weblogs or “blogs”) while acting in a JLL capacity.

b. Fraudulent, harassing or obscene messages are prohibited. No abusive, profane, or offensive language may be transmitted through JLL Information Technology Systems.

c. All messages communicated on the Internet while acting in a JLL capacity should have the Employee’s name attached. Users may not attempt to obscure the origin of any message.

d. Information published on the Internet should not violate or infringe upon the rights of others. Employees who wish to express personal opinions on the Internet shall not use JLL credentials.

e. Any information/representation pertaining to JLL shall only be released in accordance with JLL’s policies to ensure confidentiality, trade marking, copyright, stock market and other regulatory requirements have been met.

f. JLL reserves the right to filter communications and to authorize security and staff to intercept and read communications. JLL may block sites that are
Information Technology Use

deeemed as inappropriate, at its discretion. Any recorded access or attempted access of these sites may be reported immediately to the Human Resources Department for further action.

E. Technology Use

1. Users are responsible for any computer equipment assigned to you, and the Company will be entitled to make a claim against you for reimbursement if there is damage to, or loss of the equipment through personal carelessness.

2. Information technology equipment should always be protected, including the use of locking devices where necessary. Take special care of laptop computers and mobile devices to avoid loss or damage.

3. If computer equipment assigned to you is lost, stolen or damaged, the loss and the circumstances in which it happened should be reported to the head of your business unit and to the Technology Service Desk. In the case of theft, you should also report the loss to your local police station, so that a claim can be made against the Company’s insurance policy.

4. Managers are responsible for liaising with JLL Information Technology to organize equipment for each position, but JLL Information Technology is responsible for allocation of all information technology assets and the management of stock. All purchases must be carried out in accordance with Company country purchasing policies, and practices managed by JLL Information Technology.

5. All equipment that is upgraded or replaced by new equipment must be turned over to the Company and disposed of in a secure, environmentally responsible manner. Decommissioned equipment is turned over to a recycling vendor selected by the Company.

6. Terminated Employees must return all property including hardware, software, smartphones, and tablets upon leaving JLL.

7. Employees are responsible for all actions taken with their User-id, including illegal behavior.

8. Other than the exceptions set out in Section I(D)(1), passwords should not be given to anyone under any circumstance. A compromised password could be used to access JLL’s Information Technology Systems illegally. If a password is compromised, a request should be sent to the Technology Service Desk to reset it as soon as possible.

9. It is prohibited to install or play computer games on firm computers or telecommunications systems.
10. It is prohibited to try to access JLL’s Information Technology Systems or those of other companies without permission.

11. In order to preserve computer system and network security, do not access data not intended for you, log onto a server or account you are not authorized to access, probe the security of other networks or interfere with service in any way.

F. Personally Owned Devices

This section of this Policy addresses the use and control of personally owned electronic devices that connect to Information Technology Systems. Personally owned devices are any devices that are not corporately owned, e.g. devices that are not owned, purchased or reimbursed by JLL or a client, and include the following:

- Smartphones (e.g., iPhones or Androids)
- Tablet PCs (e.g., iPads, Android, Windows devices)
- Laptops
- Workstations (desktops)
- eReaders (e.g., Nook, Kindle)
- Any device that can be connected to JLL’s networks via wireless, wired, VPN, or Citrix

JLL Responsibility

1. JLL reserves the right to:
   a. manage any device with access to JLL data, including those that are personally owned;
   b. determine which device types, models, operating systems, and applications may be connected to the Company’s network and resources;
   c. determine which methods are approved for personally owned devices to connect to JLL networks;
   d. determine the level of support provided for personally owned devices and users of personally-owned devices;
   e. protect JLL data and in the case of lost or stolen devices to remotely erase the content on any device that connects to JLL networks and resources. Users who elect to connect a personally owned device to JLL Information Technology Systems agree that:
      i. if the device has been registered to the Mobile Device Management tool, where possible, only JLL information will be removed;
JLL

Corporate Governance and Compliance Policy Manual

Policy No. 14

Information Technology Use

ii. if the device is connected via ActiveSync or other method that does not enable selective deletion, a ‘wipe’ will be issued and the entire contents of the device will be deleted (including all non-JLL content that is personal to the device owner).

f. protect JLL data after an Employee or third party has terminated his or her relationship with the Company. In this case, if the device can be provided to JLL Information Technology, JLL can selectively remove all JLL data. If the device cannot be provided to JLL Information Technology prior to or immediately upon exit, the same procedure described above will apply and the entire contents of the device will be deleted.

g. refuse or remove permission for a device to connect with JLL resources and may disable access to corporate resources from any personally-owned device at any time.

2. JLL is not responsible for damage to personal devices or content due to corporate management of personally owned devices.

3. JLL is not responsible for the backup of personal data on personally owned devices.

Employee/User Responsibility

1. All JLL policies apply to users and their personally owned devices while they are connected to JLL’s networks and resources with respect to maintaining data security, adequately protecting the device and not using the device to conduct improper activities.

2. Users must not connect personally owned devices to JLL wired networks without previous approval from their reporting manager and JLL Information Technology.

3. Users may only connect personally owned devices to JLL networks using methods approved by JLL Information Technology. Contact the Technology Service Desk for approved methods.

4. Users must immediately inform JLL Information Technology if a personally owned device, used to conduct JLL business, is lost or stolen.

5. Users may be required to provide additional authentication information before being authorized to connect personally owned devices to JLL’s networks.

6. Users agree to allow security policies that enforce corporate password settings to be implemented on personally owned devices where they are to be connected to JLL’s networks.
7. Users agree to give their personally owned device to corporate managers and facilitate unrestricted access in the event of an investigation where the Company needs to collect data or perform forensics on the device or comply with a subpoena.

8. It is the user’s responsibility to backup personal data on their device.

G. Data Integrity

Information, intellectual property and innovative ideas are valuable JLL assets. These intangible assets must be appropriately managed and protected. Data of a confidential nature must be kept safe from corruption, loss or disclosure.

1. It is your responsibility to ensure the integrity of the data you have created or are entrusted with, by making sure that only current, up-to-date versions of the data are retained, or appropriate change control records are maintained.

2. In order to maintain the confidentiality and integrity of the Company’s data, you should not:
   a. Leave your computer or terminal logged on and unattended.
   b. Have your screen visible to other people when using your computer in public places, e.g., on trains or planes.
   c. Work on confidential or classified material in public places.
   d. Alter or delete data owned by another user, without their prior knowledge and consent.
   e. Leave confidential material lying unattended at a printer, photocopier or fax machine.

3. All passwords should be difficult to guess, and any compromised password must be changed immediately.

4. The firm screen saver should be used in conjunction with automatic password activation.

5. Access to Information Technology Systems is restricted to authorized personnel only.

H. Anti-Virus Protection

1. All Employees must have an approved anti-virus protection software package on their JLL issued computers. All computers that connect to JLL networks must have anti-virus software installed, even if the computer is not owned by JLL.

2. All files brought onto the Employee’s computer/network from an outside source must be scanned prior to use. Files through the email system are automatically scanned for viruses by the system.
3. Virus checking software on computers should not be disabled.

4. Some software can contain viruses or information that could damage JLL’s property. Be sure to check any potential software installation or download with JLL Information Technology. Only JLL Information Technology should install software.

5. Do not open emailed attachments if you are not expecting the message, if you do not usually correspond with the sender, if the attachment has an extension such as .exe, .vbs, or .bat, or if the message header or attachment name is vague, non-business related or gives you any cause for concern. If a message you receive falls into any of these categories, contact JLL Information Technology immediately for advice.

6. Opening of suspect email or Internet items that result in viruses may be considered negligent behavior.

7. Do not pass on information pertaining to viruses as this can cause further problems; these are usually hoaxes. Contact JLL Information Technology if in doubt.

8. Writing or distributing any form of virus is computer misuse.

9. Viruses may be covered under destruction of property laws. If you are found to have willfully caused damage, criminal charges could be filed.

I. Social Media Guidelines

Even when you are communicating your personal opinion, if your audience can associate you with JLL, you may be deemed to be acting as a spokesperson for the Company (whether you intend to or not). Social Media Guidelines have been issued and should be read in conjunction with this Policy. They apply to JLL, including LaSalle Investment Management. All users are expected to read and be familiar with the Social Media Guidelines.

III. Miscellaneous Provisions

Policy Violations

1. By virtue of accessing Information Technology Systems, each Employee agrees with and acknowledges this Policy.

2. Violations of this Policy may result in disciplinary action up to and including termination of employment. If necessary, the Company will advise appropriate legal officials of any illegal violations.

Related Global Policies

The Corporate Governance and Compliance Policies listed below form part of our wider Information Technology and Data program and can be viewed on the Company’s Intranet site.
Policy No. 14

Information Technology Use

- Policy No. 26 – Anti-virus software Policy
- Policy No. 27 - Information Classification
- Policy No. 39 – Managing Sensitive Information on Portable Devices and Removable Media
- Policy No. 45 – Global Privacy Policy
- Social Media Guidelines

In addition, some of our regional and local operations may have country or region specific Information Technology Usage policies or guidelines in order to comply with local laws and business practices that can be viewed on the relevant Regional Intranet site.

ISO 27001-2013 References

A8.1.3 Acceptable use of assets
A11.2.8 Unattended user equipment
A12.6.2 Restrictions on software installation
A13.2.1 Information transfer policies
A13.2.3 Electronic messaging

Administration of Policy

The Chief Information Security Officer and the Global General Counsel shall administer this Policy. Exceptions or changes to this Policy require the approval of the Chief Information Security Officer and the Global General Counsel.

Legal Restrictions on the Application of this Policy in Particular Countries

JLL intends this Policy to apply to all of our Employees on a worldwide basis. However, if a provision of this Policy would violate an applicable law or regulation within a particular country, then the Company will consider that such provision is void and of no force or effect as to Employees or operations within that country.

Restriction on Posting Company Policies

In order to ensure reliance on the official version of policies, this Policy shall not be copied, reproduced or posted on any Company website without prior approval of Global Legal Services.

The official version of this Policy is located on the Connect Global Policy Portal at https://jll2.sharepoint.com/CorporatePolicies/Pages/Home.aspx
Information Technology Use

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2004</td>
<td>Policy issued</td>
</tr>
<tr>
<td>January 2006</td>
<td>Minor updates to add references to blogging and to change email purging timeframe</td>
</tr>
<tr>
<td>June 2008</td>
<td>Minor updates to reference environmental responsibility</td>
</tr>
<tr>
<td>September 2008</td>
<td>Minor updates to email purging timeframe</td>
</tr>
<tr>
<td>August 2010</td>
<td>Appendix A: Social Media Guidelines added to policy</td>
</tr>
</tbody>
</table>
| July 2014  | – II.A.3 – added Instant messaging statements  
- II.A – remove email formatting  
- II.B – Email retention - remove all specific retention statements  
- II.D.2 – Computer Use – replace ‘cell phones and blackberries’ with ‘Smartphones and tablets’  
- II.E – new section on Personally-owned devices  
- II.H - Add section H reference to ‘Social Media Guidelines’ with link to the document.  
- Related Global Policies - Added  
- Appendix A – Social Media Guidelines – removed. |
| August 2015 | Minor changes – replaced ‘Jones Lang LaSalle’ with JLL. Approved by Mike Levinson |
| October 2015 | Add references to ISO27001-2013 controls. Approved by Mike Levinson 10/9/2015 |
| July 2016  | I.A – added Mobile devices to property  
I.B – removed French exclusion  
I.D.8 – added statement about exchange of non-public information  
I.E.3 – changed ‘may not’ to ‘are discouraged from’ loading non-standard software  
I.E.4 – added – right to remove non-standard software  
II – changed ‘Procedures’ to ‘Best Practices’  
II.A – added section ‘ Security Awareness’  
II.B.5 – added statement about personal email services and confidential Company messages  
II.C.3.f – added statement on internet data exchange  
II.D – removed point 2 about power consumption  
II.D.4 – restated technology purchase procedure  
II.D.14 – removed ‘must not’ statements (they were redundant)  
II.E – Personally owned devices – removed some unnecessary statements |
| May 17, 2017 | Purpose – updated definition of Information Technology Systems to include instant messaging, network access and mobile devices  
I.B (previous) – deleted because duplicative of other sections  
I.C (new) – added exception for disclosure of user-ids and passwords to JLL Information Technology  
I.C.9 – added applications and mobile applications to definition of |
Information Technology Use

“Personal Online Content”
I.E.1 (previous) – deleted subsection per comment from IP counsel
I.G – deleted because duplicative of other sections
II.A – added language about risk based assessment for security awareness
II.B.2 – deleted because duplicative of other sections
II.B.5 – added language restricting the forwarding of confidential information to personal emails
II.D.4 – deleted in its entirety as deemed out of date
II.E.2 – deleted because duplicative of other sections
II.E.10 - deleted because duplicative of other sections
Added boilerplate language on restrictions on posting company policies