TABLE OF CONTENTS

I. Statement of Policy ........................................................................................................... 2
   A. JLL Property .................................................................................................................... 2
   B. Privacy and Monitoring ................................................................................................. 2
   C. Prohibited Activities ..................................................................................................... 3
   D. Software ........................................................................................................................ 4
   E. Copyright Issues ........................................................................................................... 5

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 ............................................................................... 7
   D. Internet Use .................................................................................................................. 8
      1. Acceptable Uses of the Internet ................................................................................... 8
      2. Unacceptable Uses of the Internet ............................................................................. 8
      3. Internet Communications ......................................................................................... 8
   E. Technology Use ............................................................................................................ 9
   F. Personally Owned Devices ............................................................................................ 10

III. JLL Responsibility ......................................................................................................... 11

IV. Employee/User Responsibility ....................................................................................... 12
   G. Data Integrity .............................................................................................................. 12
   H. Anti-Virus Protection .................................................................................................... 13

V. Social Media Guidelines ................................................................................................ 14

IV. Miscellaneous Provisions ............................................................................................. 14

VI. Policy Violations ............................................................................................................ 14

VII. Related Global Policies ............................................................................................... 14

VIII. Administration of Policy ............................................................................................. 14

IX. Legal Restrictions on the Application of this Policy in Particular Countries ................ 15

X. Restriction on Posting Company Policies ...................................................................... 15

XI. Revision History ............................................................................................................ 16
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 Employees (as defined below) in order to assist them in conducting and meeting JLL’s business initiatives.

Information Technology Systems are provided to Employees for the benefit of JLL and the work it does for its clients. Employees have a responsibility to maintain and enhance JLL’s public image by using Information Technology Systems in a productive and appropriate manner.

Scope
Compliance with this Policy and procedures is mandatory for all JLL Employees, as well as temporary employees, consultants, contractors, sub-contractors (“Employees”) and (with some exceptions) third party vendors who may be involved in the transmission, processing, or storage of JLL data.

I. Statement of Policy

A. JLL Property

The Information Technology Systems and the data stored on them are and remain the intellectual property of JLL.

B. Privacy and Monitoring

1. Except as mandated by applicable local laws, JLL reserves the right without notice, to inspect, monitor or remove any JLL Information Technology Systems, and any and all data, file(s) or information created, stored, accessed, transmitted, or received by or on JLL Information Technology Systems. JLL has access to all information on all JLL Information Technology Systems. Notwithstanding the above, JLL will comply with all laws regarding 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 and in accordance with local laws, inspect, use, or disclose communications and related information without further notice or consent.

3. JLL Information Technology Systems are enabled to monitor, access, filter, retrieve, and read email, voicemail, instant messages, files and other communications composed, transmitted, reviewed, or received, to safeguard the Company against data leakage and irresponsible use. For legitimate business reasons, and to carry out our legal obligations as an employer, Employees’ use of the Information Technology Systems...
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 from its Information Technology Systems, or check Internet usage (including pages visited and searches made) on its systems as reasonably necessary in the interests of the business and in accordance with local laws, including, but not limited to, the following:
   a. to monitor whether the use of the email system or the Internet has a business requirement and is 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 any policy violations; and
   d. to comply with any legal obligation.

5. JLL reserves the right to delete any non-business or non-work-related material without prior notification in accordance with applicable local laws.

6. Except as required by applicable local laws, all communications (including text, images, audio, video and other formats) may be disclosed to law enforcement or other third parties for legitimate business or legal purposes without prior consent of the initiator or the receiver of data.

C. Prohibited Activities

1. User IDs must uniquely identify a single user. JLL Employees are prohibited from sharing User IDs and passwords except when required by JLL Technology, Data and Information Management (TDIM) teams (i) for service and maintenance purposes or (ii) when required for software installations. When a User ID or password is provided to JLL TDIM staff, it should be changed immediately after the service, support, or software installation is complete.

2. Users are prohibited from using another person’s user ID, password, PIN, or other credentials to gain access to JLL Information Technology. Users are also prohibited from attempting to guess or crack such credentials.

3. Harassment in the work environment or in any JLL work function of any kind is strictly prohibited. Voice or electronic transmissions may not contain content that may reasonably be considered offensive or disruptive to any Employee. No electronic 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.

4. 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.
5. Information Technology Systems are for business use and 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.

6. Falsifying information of any kind regarding the business, the Company or the manner that Employees represent themselves as a JLL Employee is against JLL policy.

7. Employees are explicitly prohibited from sending or forwarding unsolicited email messages from corporate email accounts (e.g. “junk mail” or “Spam”).

8. Employees may not forward or otherwise propagate chain letters, whether or not the recipient wishes to receive such mailings.

9. Employees may not exchange JLL non-public business information over systems, cloud services, or other online data exchanges that have not been approved by JLL (e.g. GoogleDocs, DropBox).

10. Personal web sites, applications or mobile applications for personal use (“Personal Online Content”) may not be established or maintained using Information Technology Systems. Personal Online Content created for JLL business must be set up in accordance with JLL procedures. JLL must approve public-facing sites hosted by the firm to ensure that they meet Company standards.

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

12. It is against JLL policy for any Employee to commit forgery, including falsifying email information including headers, addresses, signatures, etc.

13. Employees shall refrain from using their JLL email address to register for personal services such as non-business-related website accounts, non-business-related subscriptions, or other services not related to the performance of JLL duties.

D. Software

1. Only Company-approved software may be loaded on Company computers by TDIM personnel.

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

3. Employees should not load software from any source onto a JLL computer that has not been authorized by JLL TDIM. Note: in the event an Employee’s device must be restored, the device will be restored to standard build specifications, and only JLL-
provided software would be restored. If the Employee has violated this policy and loaded personal software, this software 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.

2. Failure to observe copyright or license agreements may result in disciplinary action by JLL or legal action by the copyright 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 training is available to all Employees, who are strongly encouraged to take advantage of such resources. Based on risk assessment results, security awareness training may be mandatory for some business units. Training consists of relevant curriculum and an assessment designed to demonstrate understanding of key topics and concepts. Training is updated on a regular basis to reflect changes to the Company, to technology, and to current information security practices.

B. Use of Email, Voicemail and Instant Messaging

1. The use of JLL’s Information Technology Systems, including email and voicemail, can be monitored to ensure compliance with JLL policies. Avoid messages that contain information that should not be conveyed in public. Remember that emails can be used in legal proceedings and that deleted emails are capable of being retrieved.

2. Employees may access only messages, files or programs for which they have permission.

3. Instant Messaging may only be used in the normal course of conducting Company business.
   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. Employees should not use personal email to conduct JLL business for any reason and must not forward sensitive, confidential or proprietary email from their JLL email account to a personal email account.

5. For business purposes, Employees should use enterprise bulk mail services for marketing and promotional email instead of their email address.

6. Email and Internet use is covered by laws concerning storage and transmission of obscene or hateful literature. As noted above, usage may be monitored and any misuse by Employees will not be tolerated. Violations of the law will be reported to the appropriate officials. 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, poses a risk to 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 innuendo, 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, 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. Originating 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 Policy No. 10 (Documents and Record Retention). Pursuant to this Policy, all electronic communications that are not to be saved as business records 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 maintained on other storage or removal 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 noted in Policy No. 10 (Documents and Record Retention), 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 and accessible until conclusion of the relevant dispute, as confirmed by Global Legal Services. Information covering the definition of all types of Company Records, of which email correspondence is one type, and applicable retention requirements are defined in Policy No. 10 (Documents and Record Retention).

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. Internet use should be predominantly for business reasons. JLL does permit limited personal use of the Internet and email 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 post or make disparaging comments on the Internet about the Company other than in compliance with the Company's media and disclosure policies.
   
   c. Internet search engines 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 to promote individual views not aligned with the spirit of JLL’s culture;
   
   d. to solicit non-Company business;
   
   e. where such use disrupts the operation of JLL’s network or interferes with an Employee’s productivity; or
   
   f. in any manner that violates laws.

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 information including text, audio, video, or images that he or she places, posts or transmits over the
Information Technology Use

Internet (including on personal blogs and social media) while acting in a JLL capacity.

b. Transmitting fraudulent, harassing or obscene messages is 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 or representation pertaining to JLL shall only be released in accordance with JLL’s policies to ensure confidentiality, trademarking, copyright, stock market and other regulatory requirements have been met.

f. JLL reserves the right to filter and monitor communications, and to authorize security and staff to intercept, block and read communications. JLL may at its discretion block sites that are deemed as inappropriate. 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 they are assigned. The Company is entitled to make a claim against a user 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. Employees are urged to take special care of laptop computers, mobile devices, and portable storage devices to avoid loss or damage.

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

4. Managers are responsible for requesting JLL TDIM to organize equipment for each position. JLL TDIM is responsible for allocating information technology assets and the managing stock. All purchases must be carried out in accordance with Company country purchasing policies, and practices managed by JLL TDIM.
5. All equipment that is upgraded or replaced must be returned to the Company to be disposed of in a secure, environmentally responsible manner as noted in the Technology Asset Management Standard. For access to Technology Asset Management Standard please email the Global Information Security mailbox at: IT.Security@jll.com

6. Employees who leave JLL must return all property including hardware, software, smartphones, and tablets.

7. Employees are responsible for all actions taken through the use of their User ID, including illegal behavior.

8. Other than the exceptions set out in Section I(D)(1), Employees must not share passwords with anyone under any circumstance. A compromised password could be used to access JLL’s Information Technology Systems for malicious intent. If a password is compromised, the user should contact the Technology Service Desk to lock the account and reset it as soon as possible.

9. Employees may not install or play computer games on JLL computers, laptops, or telecommunication systems.

10. It is prohibited to try to access JLL’s Information Technology Systems or those of other people or organizations without permission.

11. 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, Androids, Windows devices)
- Tablet PCs (e.g., iPads, Android, Windows devices)
- Laptops
- Workstations (desktops)
- Portable storage (thumb drives, portable hard drives)
- 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 systems and/or 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 such devices;
   e. protect JLL data and, in the case of lost or stolen devices, 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;
      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;
   h. prohibit the connection of any device to the Company network that may contain forbidden or unsafe mobile applications;
   i. prohibit the connection of any device with a jailbroken or user-modified operating system to the Company network.

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. These include 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 Security.

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

4. Users must immediately inform JLL TDIM 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 with access to JLL’s networks (e.g. passwords, passcodes, screen lock).

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, in accordance with local laws.

8. Users are responsible for backing up personal data on their device.

9. Users agree that any device with access to JLL networks or data, or storing JLL data, may only be used by the JLL employee.

**G. Data Integrity**

Information, intellectual property and innovative ideas are valuable JLL assets. These intangible assets must be appropriately managed and protected. The confidentiality, availability and integrity of this data must be maintained.

1. It is the responsibility of JLL Employees to ensure the integrity of the data they create 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, Employees should not:
   a. leave computers or terminals logged on and unattended;
   b. allow your screen to be visible to other people when using your computer in public places, e.g., on trains or planes;
   c. leave your screen visible or computer accessible to others when away from your desk;
   d. work on confidential or classified material in public places;
   e. alter or delete data owned by another user, without their prior knowledge and consent;
   f. leave confidential material lying unattended at a printer, photocopier or fax machine; or
   g. leave confidential, valuable, or sensitive information lying unattended and accessible in a personal workspace, such as a desk or meeting room.

3. All passwords must meet complexity requirements as outlined in the User Account Management Standard. For access to the User Account Management Standard please email the Global Information Security mailbox at: IT.Security@jll.com Compromised password must be changed immediately. The Technology Service Center should be notified of any account compromise.

4. Screen savers should require a password in order to unlock and access a computer or device.

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

6. Any suspected breaches of data integrity should be reported to the Technology Service Desk and the appointed Legal & Compliance Representative in accordance with Policy No. 28 – Data Breach and Information Security Incident Response.

H. Anti-Virus Protection

1. All Employees must have approved anti-virus protection software 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 and networks from outside sources must be scanned prior to use. Files sent through the email system are automatically scanned for viruses.

3. Virus checking software on computers shall not be disabled.
4. Some software can contain viruses or malware that could infect and damage JLL’s assets. Only approved JLL software/applications should be installed and installation should be performed by TDIM.

5. Do not open emailed attachments from unfamiliar sources if you are not expecting the message, or 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, do not open the file. If a message you receive falls into any of these categories, contact the Technology Service Desk immediately for advice.

6. Opening of suspect email or Internet items that result in spreading viruses may be considered negligent behavior and subject Employees to disciplinary action.

7. Employees should not knowingly pass on information pertaining to viruses as this can cause further problems. These are usually hoaxes. Contact TDIM if in doubt.

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

9. Viruses may be covered under destruction of property laws. A user found to have willfully caused damage may be subject to criminal charges.

III. Social Media Guidelines

Even when 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). All Employees (including LaSalle Investment Management) are expected to read and be familiar with the Social Media Guidelines.

IV. Miscellaneous Provisions

Policy Violations

1. All JLL Employees who access Information Technology Systems are required to agree with and acknowledge 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 officials of any violations of the law.

Related Global Policies

The Corporate Governance and Compliance Policies listed below form part of our wider Technology, Data and Information Management (TDIM) program and can be viewed on the Company’s Intranet site.

- Policy No. 26 – Anti-virus software Policy
Policy No. 14

Information Technology Use

- Policy No. 27 - Information Classification
- Policy No. 28 – Data Breach & Information Security Incident Response
- Policy No. 39 – Managing Confidential Information on Mobile Devices and Removable Media
- Policy No. 45 – Global Privacy and Data Protection 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 to comply with local laws and business practices. These are available on the relevant Regional Intranet site. Where there may be a difference in policies or standards, the regional policy or standard may be more relevant.

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 and processes
A13.2.3 Electronic messaging

Administration of Policy

The Global 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 our Employees worldwide. However, if a provision of this Policy would violate a law or regulation in a particular country, the Company will consider such provision void and of no force or effect on Employees or operations in 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.
Policy No. 14

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
| August 17, 2018 | - Making minor revisions to section I.B and I.C to acknowledge local privacy laws  
- Adding G.6 (reporting data breaches)  
- Including reference to restrictions on forwarding confidential information to personal email address  
- Including reference to Policy No. 28  
- General drafting changes for clarity  
- Approved by Mike Levinson, CISO |

“Personal Online Content”  
I.E.1 (previous) – deleted subsection per comment from IP counsel  
L.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