ENTERPRISE INFORMATION SECURITY POLICY

Approval and Revision History Table:

<table>
<thead>
<tr>
<th>ISSUE 5.0:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why: New Release</td>
</tr>
<tr>
<td>Changes and updates due to an annual policy review and audit findings</td>
</tr>
<tr>
<td>Impact on Users:</td>
</tr>
<tr>
<td>Users will no longer be permitted to use removable media for computer backups. Instead company provided storage will be provided to all users to backup their data.</td>
</tr>
<tr>
<td>Change Details:</td>
</tr>
<tr>
<td>V5: Changed document reference #s, changed approvers to remove Steve Wenc and add Brian Monks, &amp; added IT BU reviewers, modified document scope to include &quot;laboratories/engineering workstations&quot;, Changed definition in 3.5 and added information in 3.5.4 on restricted data, changed 4.1.3 around portable media storage and added &quot;and while at rest&quot; to 4.2.2 Data Encryption section. Also modified 4.3.1 and 4.3.2 for intranet and extranet access. In 5.1 for physical security, added cellphone/camera usage in secure labs. Removed the use of lanyards in 5.2.1 and edited 6.0, the applicable documents section to keep only those that are pertinent to this policy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Security Process Owner (Owner - Originator)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Schaub - 2015/4/15</td>
</tr>
<tr>
<td>Information Security Director (Approver)</td>
</tr>
<tr>
<td>Robert Jamieson-2015/4/7</td>
</tr>
<tr>
<td>Information Technology Director (Approver)</td>
</tr>
<tr>
<td>Thomas Boxrud-2015/4/29</td>
</tr>
<tr>
<td>Information Technology Director (Reviewer)</td>
</tr>
<tr>
<td>Kent Walker</td>
</tr>
<tr>
<td>Information Technology Director (Reviewer)</td>
</tr>
<tr>
<td>EeSeng Koh</td>
</tr>
<tr>
<td>Information Technology Director (Reviewer)</td>
</tr>
<tr>
<td>Edward Rich</td>
</tr>
<tr>
<td>Information Technology Manager (Reviewer)</td>
</tr>
<tr>
<td>Steve Wong</td>
</tr>
<tr>
<td>Information Technology Lead (Reviewer)</td>
</tr>
<tr>
<td>Rich Martin</td>
</tr>
<tr>
<td>Information Technology Lead (Reviewer)</td>
</tr>
<tr>
<td>Microsoft Enterprise Services Lead (Reviewer)</td>
</tr>
<tr>
<td>Sandi Glazebro</td>
</tr>
<tr>
<td>SVP Chief Information Officer (Approver)</td>
</tr>
<tr>
<td>Christian Anschuetz-2015/5/19</td>
</tr>
<tr>
<td>Information Technology Director (Approver)</td>
</tr>
<tr>
<td>Andreas Geil</td>
</tr>
<tr>
<td>Information Technology Director (Reviewer)</td>
</tr>
<tr>
<td>Nirav Patel</td>
</tr>
<tr>
<td>Information Technology Director (Reviewer)</td>
</tr>
<tr>
<td>Edward Rich</td>
</tr>
<tr>
<td>Information Technology Manager (Reviewer)</td>
</tr>
<tr>
<td>Sankalp Mahajaran</td>
</tr>
<tr>
<td>VP Global Security &amp; Brand Protection (Approver)</td>
</tr>
<tr>
<td>Brian Monks-2015/6/2</td>
</tr>
<tr>
<td>Information Technology Director (Approver)</td>
</tr>
<tr>
<td>Tim Dalgren</td>
</tr>
<tr>
<td>Information Technology Director (Reviewer)</td>
</tr>
<tr>
<td>Microsoft Enterprise Services Lead (Reviewer)</td>
</tr>
<tr>
<td>Sandi Glazebro</td>
</tr>
<tr>
<td>Information Technology Director (Approver)</td>
</tr>
<tr>
<td>Ted McNally</td>
</tr>
<tr>
<td>Information Technology Director (Reviewer)</td>
</tr>
<tr>
<td>EeSeng Koh</td>
</tr>
<tr>
<td>Information Technology Director (Reviewer)</td>
</tr>
<tr>
<td>Edward Rich</td>
</tr>
<tr>
<td>Information Technology Manager (Reviewer)</td>
</tr>
<tr>
<td>Sankalp Mahajaran</td>
</tr>
<tr>
<td>Information Technology Director (Reviewer)</td>
</tr>
<tr>
<td>Edward Rich</td>
</tr>
<tr>
<td>Information Technology Manager (Reviewer)</td>
</tr>
<tr>
<td>Sankalp Mahajaran</td>
</tr>
<tr>
<td>Information Technology Director (Reviewer)</td>
</tr>
<tr>
<td>Edward Rich</td>
</tr>
<tr>
<td>Information Technology Manager (Reviewer)</td>
</tr>
<tr>
<td>Sankalp Mahajaran</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS

1.0 PURPOSE ........................................................................................................................................... 3
2.0 SCOPE .................................................................................................................................................. 3
3.0 RESPONSIBILITY ................................................................................................................................ 3
   3.1 UL’s Chief Security Officer ................................................................................................................. 4
   3.2 UL’s Information Security Director .................................................................................................... 4
   3.3 The Internal Audit Team .................................................................................................................... 4
   3.4 Information Owners ............................................................................................................................ 4
   3.5 Data Stewards ................................................................................................................................... 4
   3.6 Management ..................................................................................................................................... 5
4.0 INFORMATION SECURITY POLICY .................................................................................................... 5
   4.1 Usage Controls ................................................................................................................................. 5
   4.2 Electronic Communications Policy (Refer to document 00-IT-P0408) .............................................. 5
   4.3 Intranet and Extranet Access ............................................................................................................. 6
   4.4 Data Management ............................................................................................................................. 6
   4.5 Enterprise Backup Data Retention .................................................................................................... 8
   4.6 Use of Computers and Computer Software ...................................................................................... 8
   4.7 Exclusive Ownership of Developed Material .................................................................................. 8
   4.8 Anti-Malware .................................................................................................................................. 9
   4.9 Wireless or Portable Computer Device ............................................................................................ 10
   4.10 Laptop and Desktop Computer Devices .......................................................................................... 10
   4.11 Network Security ............................................................................................................................ 10
   4.12 Remote User Access ....................................................................................................................... 10
5.0 ENVIRONMENTAL AND PHYSICAL CONTROLS ............................................................................ 11
   5.1 Physical Security ............................................................................................................................. 11
   5.2 Compliance ....................................................................................................................................... 12
6.0 APPLICABLE DOCUMENTS ................................................................................................................ 12
APPENDIX - DEFINITIONS .................................................................................................................... 13
1.0 PURPOSE

Protecting confidential UL and customer information is critical to the success of UL’s business and our Public Safety Mission. UL’s customers provide us with confidential and restricted information that we use to provide our services. UL also creates its own proprietary, confidential, and restricted information. Everyone at UL is responsible for safeguarding this information.

UL’s Information Security Program and Policy is based on three core principles:

- **Confidentiality** - preventing the disclosure of proprietary, confidential, or restricted information to unauthorized individuals or systems
- **Integrity** – maintaining and assuring the accuracy and consistency of data in UL’s systems
- **Availability** – providing access to information systems and data when and where authorized users need them

This Policy is part of UL’s overall Information Security Program. The Policy has been reviewed, approved and endorsed by UL’s management. It establishes a framework for preserving the confidentiality, integrity and availability of information on UL’s information systems and in UL’s laboratories/engineering spaces. The Policy also establishes a framework for protecting UL’s systems from theft, abuse, misuse or damage. Detailed standards, guidelines and operating procedures provide additional information for implementing the Policy. Those supporting materials are referenced in this Policy.

2.0 SCOPE

All UL employees, contractors, sub-contractors, joint ventures, board members, and vendors must comply with this Policy. This Policy applies to all of UL’s businesses, functions, services and systems. It applies to all UL computers, peripherals, mobile computing devices, datacenters, networks, applications, web portals, databases, programs, IT infrastructure, laboratories/engineering workstations, and all information content including physical copies of information.

3.0 RESPONSIBILITY

All UL employees, contractors, sub-contractors, joint ventures, board members, and vendors, must comply with this Policy. Additionally, all UL employees, contractors, sub-contractors, joint ventures, board members, and vendors are responsible to safeguard all customer & UL information and the physical assets that electronically or physically store that information in accordance with this Policy and immediately report any disclosure of protected information to unauthorized parties to their immediate supervisor.

Violations of UL policies, practices, procedures (including the Enterprise Information Security Policy) and applicable laws and regulations, may result in disciplinary action, up to and including termination of employment. Local law, policies and practice will govern the specific disciplinary process, including criminal prosecution, where applicable. Additionally, some individuals and groups have specific responsibilities under this policy as described below:
3.1 UL’s Vice President of Global Security and Brand Protection is responsible for establishing and administering Information Security policies, standards, guidance and procedures.

3.2 UL’s Information Security Director is responsible for implementing the Information Security Policy and program and for the direct supervision of the Information Security Team.

3.2.1 The Information Security Team is responsible for investigating and responding to information security breaches and other information security incidents, monitoring enterprise information security, developing and deploying system security measures, and providing support and guidance to help employees fulfill their responsibilities under this Policy.

3.3 The Internal Audit Team is responsible for conducting audits that measure compliance with this Policy and working with UL’s outside auditors, where appropriate, to assess compliance with this Policy.

3.4 Information Owners are the senior IT Directors or leaders assigned to Business Units or Functions who act on behalf of the senior executive of that organization. Information Owners are responsible for:

3.4.1 Implementing UL’s data classification policy for their Business Unit or Function as described in Section 4.4 of this Policy
3.4.2 Defining the types and levels of data access for the job roles in their Business Unit or Function consistent with UL’s data classification policy
3.4.3 Ensuring that their Business Unit or Function follows UL’s IT governance process for change management of the Business Unit’s or Function’s applications and data storage systems and take appropriate action to make sure that such applications and data storage systems meet UL’s information security requirements
3.4.4 Annually assess the security of the processes, applications, databases and information in their Business Unit or Function in accordance with this Policy
3.4.5 Following UL’s Solution Delivery Life Cycle process for all systems and applications implementations (Refer to 00-IT-S0405)

3.5 Data Stewards are the IT, Engineering, or Laboratory personnel directly responsible for a database or other information source or system. Data Stewards are responsible for:

3.5.1 Implementing the data classification and access policies established by the Information Owners
3.5.2 Implementing the backup, data retention and maintenance schedules established by UL IT or Information Owners
3.5.3 Applying all security updates and vulnerability management (“patching”) for their database or system
3.5.4 Insuring that all “Restricted” information is appropriately stored in secured containers or on segregated networks per Security Guidance document

Copyright© UL LLC. All rights reserved. May not be reproduced without permission. UL PROPRIETARY AND CONFIDENTIAL. FOR UL INTERNAL USE ONLY. This document is controlled and has been released electronically. The version on the UL intranet is the up-to-date document. Hard copies are uncontrolled and may not be up-to-date. Users of hard copies should confirm the revision by comparing it with the electronically controlled version.
3.6 Management are all leaders within UL’s family of company’s, contractors, sub-contractors, joint ventures, board members, and vendors. Managers are responsible for:

3.6.1 Ensuring that the people within their organization understand and follow this policy and referenced work instructions

3.6.2 Ensuring that the people within their organization appropriately protect information assets and physical property

3.6.3 Immediately reporting any disclosure of protected information to unauthorized parties to UL’s Information Security team

4.0 INFORMATION SECURITY POLICY

4.1 Usage Controls

4.1.1 Authentication

UL employs several different types of user authentication to confirm identity online including physical authentication tools, such as biometrics. These are based on who the user is (e.g., biometrics), what they have (e.g., certificate/smart card/badge), and what they know (e.g., password). All UL employees, contractors, sub-contractors, joint ventures, board members, and vendors must safeguard their authentication sources and must not disclose those authentication sources to any outside parties. If any person loses an authentication tool or their password information is compromised, they must immediately report the loss to UL’s Service Desk or UL’s Information Security Team. All applications used by UL’s companies/legal entities must have their identities and access management controlled by the corporation’s Identity and Access Management (IAM) System.

4.1.2 Passwords

UL requires strong, complex passwords to protect our systems. For password requirements, refer to UL’s Password Policy (00-IT-P0407 & Password Guidance document).

4.1.3 Portable Media (including USB hard drives and flash memory)

All portable media must be scanned for malware before use (Refer to document on Malware Management). Portable media, cell phones, tablets, any device that can copy, photograph, or electronically capture images are prohibited from all Confidential and Restricted areas. Portable media must also be protected according to UL’s data classification policy as described in Section 4.4 of this Policy. Portable Media will not be used for computer backups and storage of confidential, proprietary, or restricted information without manager approval. Backup copies of data will only be created on UL provided storage devices/systems.

4.2 Electronic Communications Policy (Refer to document 00-IT-P0410)

4.2.1 Email Storage

UL’s Email system is not the appropriate place to store confidential, proprietary, or restricted information. Such information must be stored in the appropriate database or application based on its business purpose. For example, customer product information should be stored in the correct database, such as DMS for Product Safety. Electronic communications containing information serving a UL business purpose will also be managed according to the data classification policy described in Section 4.4 of this Policy.
4.2.2 **Data Encryption**

All information classified as confidential, proprietary, or restricted must be encrypted while being electronically transmitted and while at rest. If any personnel are unsure whether certain information is confidential, proprietary, or restricted, assume that it requires encryption (for additional information refer to the Security Guidance Document).

4.2.3 **Email or “web mail” access on shared computers or kiosk machines**

All personnel who access email/web mail from any non-UL computer, such as a hotel business center or library computer must take the following steps to protect their identity:

- Do not check “remember credentials”
- Log out of the session before leaving the computer
- Delete browser history before leaving the computer (for additional information refer to the Security Guidance Document)

4.2.4 **Instant Messaging (IM) or Chat.** UL’s approved IM service is a secure, internally-hosted instant messaging system that can be used for both internal and external collaboration. Non-UL IM and Chat tools may not be secure and must not be used to transmit confidential, proprietary, or restricted information.

Employees must not open or accept IM attachments transmitted through a public IM service. All attachments/files must be sent via UL e-mail system or UL’s approved IM service.

4.3 **Intranet and Extranet Access**

4.3.1 The UL IT Department must authorize all connections between UL’s network(s) and the internet from UL office locations. Non-IT personnel must not set up their own internet connections between the UL network and the internet. Guest wireless networks are for the convenience of UL’s customers while on site and the passwords to access these systems will not be shared with any party not directly engaged with or doing business with UL.

4.3.2 UL reserves the right to block access to web sites that are deemed dangerous, malicious, undesirable, and/or not appropriate for business purposes.

4.3.3 Laboratories processing “Restricted” information will not have access to the internet and all server ports must be closed unless specifically authorized by the Information Security Director.

4.4 **Data Management**

4.4.1 **Data Classification.**

All UL employees, contractors, sub-contractors, joint ventures, board members, and vendors are responsible to classify information in UL’s systems, including customer information as one of the following:

- **Public Data/Information** is Data/Information commonly known to the general public or available from public sources
  - Data classified as “Public Data/Information” does not require special protection however does possess a duty of care to insure the integrity of the data.
• **Proprietary Data/Information** is content created from UL’s interactions with its customers or other sources that is not publicly available or known from any other source
  
o Data classified as “Proprietary Data/Information” requires special protection and access restrictions from unintentional or unauthorized disclosure to any party other than those specifically authorized to view the information.

• **Confidential Data/Information** is either customer or UL data/information content that is not publically available and includes: (a) business and marketing plans and financial information; (b) plans, designs, sketches, and prototypes for products and services; (c) engineering and technical information such as software, test processes and methodologies, data, and test equipment and fixtures; (d) trade secrets; and (e) information concerning the disclosing Party’s customers, business partners, or affiliates and their products or services or any other information from our customers that has been designated as confidential.
  
o Data classified as “Confidential Data/Information” requires separate and discrete protection and access restrictions from unintentional or unauthorized disclosure to any party other than those specifically authorized to view the data/information.

• **Restricted Data/Information** is customer or UL data/information content that requires access to be granted on a “need to know” basis only. This data uses the same discrete protection and access protection as “Confidential Data/Information” but with additional restrictions on the persons who may gain access to the data/information.

4.4.2 Default Data Classification

All customer data will be classified by default as confidential information unless the the data owner reclassify’s it to Public or Restricted when created.

UL generated data is classified as proprietary information unless the data owner reclassify’s it to Public or Restricted when created.

Data may be reclassified at anytime as appropriate. Data reclassification is the responsibility of the data owner.

4.4.3 Data/Information Disposal

All data/information intended for disposal must be properly shredded and/or deleted. Data on magnetic media such as hard disks, tapes, CDs, or removable storage devices shall be “destroyed” by physical shredding, multiple reformatting (three or more times), or degaussing (for additional information refer to the [Security Guidance Document](#)). Physical (i.e. printed) copies of customer’s “Confidential or Restricted” information and associated physical samples will either be returned to the customer or destroyed by physical shredding.

4.4.4 External Disclosure of Confidential, Proprietary, or Restricted Information

4.4.5 All confidential, proprietary, or restricted data/information (including raw test data) transmitted outside the UL network with customers, sub-contractors, contractors, vendors or...
partners must be encrypted prior to it being sent to ensure it is not intercepted by unauthorized parties (for additional information refer to the Security Guidance Document). Laboratories processing “Restricted” information will also protect against the unintended transmission of electronic data to unauthorized parties (ex. RF Shielding). External Disclosure of Security Information

Information regarding security measures for information systems and networks is classified as restricted and must not be disclosed to unauthorized persons unless approved by the Information Security Director (for additional information refer to the Security Guidance Document).

4.5 Enterprise Backup Data Retention

4.5.1 Server backup retention of data is governed by the HANDLING DATA BACKUP AND RETENTION POLICY, 00-IT-P0829. At a minimum, the Enterprise backup data retention process will incorporate the following:

- Only approved, standardized backup software will be used
- Access to backed up data will be restricted in accordance to the data classification policy
- Backed up data will only be stored offsite with approved vendors

All data storage must comply with applicable export controls.

4.6 Use of Computers and Computer Software

All UL employees, contractors, sub-contractors, joint ventures, board members, and vendors who use UL issued computers, tablets, or smart devices or who access UL systems from their own devices must read, understand, and comply with UL’s Enterprise Use of Computers and Computer Software Policy (Policy 00-IT-P0409).

UL computers will not to be issued to any customers, other outside organizations, or individuals (such as preferred partners or contractors) for connections to UL’s systems and applications that circumvent UL’s access controls. All users of UL’s Information Systems and applications are required to have an unique ID provisioned within UL’s Identity and Access Management system to access UL’s computing systems and applications. Lab test equipment may be exempt from this requirement upon approval by UL’s Information Security Director.

4.6.1 Non-UL Owned Computers

Non-UL owned computers shall not be connected into UL’s network without a signed Non-Disclosure Agreement (NDA) by the using party. Use of the wireless guest network is provided in most UL facilities for visitor internet access.

4.7 Exclusive Ownership of Developed Material

UL owns exclusive rights to patents, copyrights, inventions or any other intellectual property developed by its employees. All programs and documents produced or provided by employees for the benefits of UL are the property of UL and the latter reserves the right to access and the use of the information.
4.8 Anti-Malware

4.8.1 Malicious Software / Computer Virus Protection

4.8.1.1 Servers

UL’s systems must have a functioning, updated to the latest version anti-virus client running on them at all times. Employees, contractors, sub-contractors, vendors, support personnel, and partners are prohibited from attempting to defeat or circumvent this application.

4.8.1.2 Workstations

All UL computer assets (desktop, laptop, or other network connected device) must run the current release of UL’s standard virus scan application. All UL employees, contractors, sub-contractors, joint ventures, board members, and vendors are responsible to insure that this application is not disabled or circumvented.

The only exceptions to this policy are in special cases where laboratory computers/test equipment requires that their anti-virus be disabled to perform necessary tests. In all cases, these exceptions will be behind a separate firewall or will be running a software firewall or will be on a separate virtual local area network (VLAN) to maintain their isolation from the remainder of UL’s systems and to isolate these systems from the other production systems.

4.8.2 Cloud Storage Solutions

Due to the increased vulnerability of confidential, proprietary, or restricted data being compromised, intercepted, or stolen when stored on removable media or in cloud storage locations, these solutions will only be used if preapproved by management and the Information Security Director. Any removable media or cloud storage solution must fully comply with the Enterprise Cloud Computing Policy and this policy including but not limited, to hard disk encryption or data encryption at rest (for additional information refer to Enterprise Cloud Computing Policy 00-IT-P0853).

4.8.3 Removable Media

UL’s standard virus protection defenses analyze files for the presence of malicious content when they are accessed. Additionally, full virus scans are periodically run on all UL workstations. Because the standard virus protection defense does not scan portable media such as USB flash drives by default, such removable media devices or documents that are downloaded from cloud storage solutions must be scanned for viruses before use (Refer to document on Malware Management).
4.9 **Wireless or Portable Computer Device**

Wireless and mobile computer devices, such as mobile phones, smartphones and tablets are not considered to be secure computing devices. Additionally, these devices can be easily lost or stolen. Confidential, proprietary, or restricted information stored on these devices must be password protected (encrypted using approved encryption methods) and the devices themselves must be password protected. The Information Security Department may block unauthorized activity on wireless networks in the event of an security incident. The following precautions also must be taken:

- Devices should never be left unattended in public areas
- All devices should be carried as hand luggage when travelling unless it is prohibited due to airline policy / security or local law or regulation
- Password/unlock feature must be enabled

UL reserves the right to remotely wipe any mobile computing device of any confidential, proprietary or restricted data.

4.10 **Laptop and Desktop Computer Devices**

All company-owned laptop and desktop computers must have full disk encryption. UL’s PC Services team will ensure that all laptops and desktops have full disk encryption when they are issued (for additional information refer to Information the Security Guidance Document). All UL employees, contractors, sub-contractors, joint ventures, board members, and vendors must immediately report a lost or stolen UL-owned laptop computer or other portable device to their immediate supervisor and the service desk to disable any unauthorized UL data synchronization.

4.11 **Network Security**

All entry and exit access points to the UL network must be protected by a firewall approved by UL’s Network & Security Team.

External connections to information systems must be protected via the company’s enterprise Identity & Access Management (IAM) system. All network-connected computers and mobile devices that contain proprietary, confidential, or restricted data/information must also utilize UL’s IAM system. Information systems must also be equipped with a screen/password lock after a period of inactivity and shared systems must use a session closing mechanism that automatically shuts down the user session after a given period of inactivity (a maximum of eight hours; exceptions to this can be granted by the Information Security Director as per paragraph 4.8.1.2 above).

All changes to the network will be recorded in UL’s change management system and carried out by authorized personnel from UL’s Enterprise Infrastructure Services team. For the purpose of data classification, network information is always classified as “restricted” and shall not be disclosed without prior approval from the Information Security Director.

Exceptions to the network security policy that may be necessary for business operations must be approved by the UL’s Information Security Director.

4.12 **Remote User Access**

UL employees, contractors, sub-contractors, joint ventures, board members, and vendors and any other external user shall only use UL’s defined remote access solutions to remotely connect to UL’s networks. Wireless access points and similar devices will not be connected to the UL internal network without prior authorization by UL Enterprise Infrastructure Services.
Remote access connections will use two-factor authentication to the UL network. Customers, partners and vendors requiring remote access to UL’s systems will be provisioned within UL’s IAM system. Any non-UL asset remotely connecting to UL must have an active, up-to-date, and functioning anti-virus client. This anti-virus client will be verified by the UL’s Service Desk before issuance of the certificate from UL’s certificate authority.

All DSL lines, dial-up modems, internet connection technologies for third party access not using UL’s firewalls will be disabled unless otherwise approved for specific use by the Information Security Department.

5.0 ENVIRONMENTAL AND PHYSICAL CONTROLS

Access to server rooms, data centers, or work areas containing proprietary, confidential, and/or restricted data/information is restricted and will only be granted to UL employees, contractors, sub-contractors, joint ventures, board members, vendors, and any other external persons on a need-to-know basis (for additional information refer to the Security Guidance Document). Confidential, proprietary, and restricted data/information including data/information contained on hard disk drives, magnetic tapes, CD/DVDs must be protected against unauthorized disclosure, and shall be secured in locked facilities when not being used during non-working hours or when authorized personnel cannot be present.

Access to offices and work areas containing confidential, proprietary, or restricted data/information is restricted and must only be granted to UL employees, contractors, sub-contractors, joint ventures, board members, and vendors on an “need to know” basis.

5.1 Physical Security

All confidential, proprietary, and restricted data/information must be physically protected and stored in locked containers or rooms to prevent unauthorized disclosure. All personnel entering areas containing Restricted information must leave their cell phones or any device capable of capturing visual images outside of that area.

5.1.1 Restricted Access to Computer, Telephone and Network Facilities

IT facilities such as network switches, routers, firewalls, voice system PBX, and other server equipment must be located in a locked-access controlled room (for additional information refer to the Security Guidance Document).

5.1.2 Location of Computer, Telephone and Network Facilities

Data centers, server rooms, telephone/PBX, and network facilities must not have signage indicating their location and will be constructed to protect against forced access, fire or water damage, or other likely threats and risks. Display screens for servers or terminals that handle Proprietary, Confidential, or Restricted data/information will be positioned so that they cannot be easily viewed by persons walking by or waiting outside the secure area.

5.1.3 Visitor Management

Personnel accessing data centers, server rooms, or work areas containing confidential, proprietary, and restricted data/information will be escorted by cleared personnel at all times and will be required to sign a visitor log and visitor release form to record their entry and exit into and out of the secure area. All visitors to a secure area must leave any cell phone or device capable of recording visual images outside the visited area. Visitors to the corporate data center are required to sign a log that is kept outside the secured area and monitored by.
data center personnel and video cameras (Please refer to the Security Guidance Document for the appropriate procedure doc).

5.1.4 Tailgating - Piggybacking
Tailgating or piggybacking is the act of entering a facility or grounds closely behind another person without supplying the necessary keycard or appropriate authentication.

Tailgating or piggybacking is prohibited within all UL facilities and location by all personnel governed by this policy and any other third parties. All personnel governed by this policy are expected to question/stop acts of tailgating or piggybacking and report the activity to responsible site management or security personnel.

5.2 Identification

5.2.1 Badges
All personnel governed by this policy are required to prominently display their UL issued identification at all times while present within UL facilities/properties. Exceptions may be granted by local responsible management when wearing the lanyard can pose a safety hazard while operating machinery.

All visitors to UL facilities are required to display a temporary issued badge in full view while on UL properties.

5.3 Compliance

5.3.1 UL will periodically conduct unannounced security audits to ensure compliance with all applicable security policies and procedures. Employees who, by negligence or design, violate security policies may be subject to disciplinary action.

UL’s Information security policies will additionally comply with applicable legislation, such as laws regarding data protection, access to information, protection of personal information, and electronic documents.

UL reserves the right to change or modify this policy at any time.

Additional information can be found within the Information Security Process documentation (00-IT-S0484).

6.0 APPLICABLE DOCUMENTS

<table>
<thead>
<tr>
<th>Doc. #</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-IT-P0403</td>
<td>UL IT Management Policy</td>
</tr>
<tr>
<td>00-LE-P001</td>
<td>Standards of Business Conduct</td>
</tr>
<tr>
<td>00-IT-P0407</td>
<td>Enterprise Password Policy</td>
</tr>
<tr>
<td>00-IT-P0410</td>
<td>Enterprise Electronic Communications Policy</td>
</tr>
<tr>
<td>00-IT-P0409</td>
<td>Enterprise Use of Computers and Computer Software</td>
</tr>
<tr>
<td>00-QA-P0026</td>
<td>Global Records Policy</td>
</tr>
<tr>
<td>80-HR-P0001</td>
<td>U.S. Employee Manual</td>
</tr>
<tr>
<td>00-IT-P0408</td>
<td>Malware Management</td>
</tr>
<tr>
<td>00-IT-P0409</td>
<td>Password Guidance</td>
</tr>
<tr>
<td>00-IT-P0410</td>
<td>Security Guidance Document</td>
</tr>
</tbody>
</table>
APPENDIX - DEFINITIONS

**Authentication** is the process of identifying yourself to a system in order to gain access. The authentication process validates the credentials supplied by the user (username, password, fingerprint, and so on) such that the individual is granted the appropriate rights based on their profile.

**Cloud computing** refers to services provided by external vendors for hosting and storing electronic data on the internet.

**Company Asset** includes but is not limited to its Information Technology systems, hardware, software and network.

**Confidential** is a term used to describe data, documents, or other material that, if disclosed, could potentially compromise the company's operational, competitive, or financial position, public image, reputation, customer confidence, and/or result in legal and contractual liability to UL.

**E-mail Spoofing** is a method used to make an e-mail appear as if it came from a sender other than the actual sender. It is often an attempt to trick the user into making a damaging statement or releasing sensitive information, such as passwords.

**Executable File** is a file that contains code that is capable of being executed or run on a computer.

**Information Asset** is considered to be computer-based information or data in any form, including physical, electronic, and magnetic created or used during the conduct of business for the company.

**Malicious Software** is a program or part of the program intended to disrupt, alter or destroy all or part of the logic elements essential to the operation of information systems. These programs can be divided into four classes: computer viruses, worms, Trojan horses and logic bombs.

**PBX** (private branch exchange) is a telephone exchange that serves a particular business or office, as opposed to one that a common carrier or telephone company operates for many businesses or for the general public.

**Remote Access** is the way to access UL computer & network resources outside the office.