

## ACCEPTABLE USE POLICY (“AUP”)

### FOR

### CONNECTIONS TO LIMITED BRANDS, INC.’s (“LBI”) NETWORK

THIS SITE EXPLAINS YOUR LEGAL OBLIGATIONS AND LBI’S RIGHTS RELATED TO THE USE AND PROTECTION OF LBI’S NETWORK. PLEASE READ CAREFULLY.

#### *I. Definitions*

“You” or “Your” as used throughout this document means all LBI associates, authorized and potential consultants, contractors and subcontractors (collectively “contractor”), and all employees, agents and representatives of each.

“Connection” as used throughout this document means any data connection established between LBI’s computer Network and You (collectively “Connecting Party”), whether remotely from equipment located at Connecting Party’s data facility and/or from equipment of Connecting Party or that LBI has loaned Connecting Party located at an LBI facility, to provide Connecting Party with access and use to selected portions of the Network or to allow Connecting Party a data Connection with third party Networks.

“Network” as used throughout this document means all program interfaces, structures, functionality, computer code, databases and the like, wired or wireless computers, servers, routers, cables and other equipment which can transmit or store data electronically, which form LBI’s local and worldwide area Networks, whether physical or virtual.

#### *II. Scope*

***Objective of this Policy: To protect intellectual and other property interests of LBI and to prevent the use of LBI technology in a manner that adversely affects job performance, disrupts others or compromises LBI data.***

LBI is committed to enhancing the ability of associates and contractors to perform their duties and increase their productivity through the use of technology assets. Careless, inappropriate or unethical use of technology assets can have unintended consequences. Individuals must use discretion and judgment consistent with LBI values when using technology assets.

Violations of the following policies – no matter how trivial they may seem at the time – may be harmful to the interests of LBI and will be treated accordingly. Violations may result in appropriate disciplinary action, up to and including termination of employment or contracted services, recovery of damages, filing of criminal charges and termination of the connection to technology assets or network resources.

Associates or Contractors who become aware of a violation of the acceptable use policy are encouraged to report the incident to notify LTS IT Security Management (LTSsecurity@limitedbrands.com) or the ethics hotline (888-884-7218 or generalcounsel@limitedbrands.com). Exceptions to the acceptable use policy due to job responsibilities will be reviewed by General Counsel and LTS IT Security Management. Exception requests must be submitted via the policy exception option within the request management system available on GettingToNext.com.

#### *III. Electronic Equipment/Information and Communications*

LBI *may* provide associates and contractors with access to technology assets. Supplied technology assets are intended for business-related matters but may also be used within reason to address occasional and necessary personal needs. Associates or contractors must not connect their personal owned technology assets to the company network. Technology assets include but are not limited to:

- Blogs
- Instant messaging
- Network access and network resources
- Network devices such as switches, hubs, wireless network equipment
- Electronic mail (e-mail)
- Voice mail
- Desktop computers

- Fax machines
- Telephones
- Computer servers and printers
- Internet access
- Remote access connectivity
- Mobile devices such as laptops, mobile POS, RF guns
- Mobile messaging devices such as pagers, mobile phones, Windows CE devices, BlackBerry, iPhones.
- Mobile storage devices such as disk drives, tapes, USB thumb drives, CD burners, iPods.

**By using LBI information services, every associate agrees he or she will not at any time use the company information or technology assets in the following manner:**

- (a) To further the business activity of any entity other than LBI and its affiliates;
- (b) To conduct a job search (except as part of a company authorized outplacement process);
- (c) To engage in activities for personal financial profit other than acceptable transactions involving company benefits such as exercising stock options or investments decisions involving the company's SARP.
- (d) To knowingly use or spread (i.e., access, download, upload, transmit) the following material:
  1. Material that violates LBI equal employment opportunity or non-harassment policy or its temporary worker statement of compliance – for example, material that contains derogatory racial or gender related comments, pornographic or obscene materials or derogatory religious comments;
  2. Information that is knowingly, recklessly or maliciously false;
  3. Copyrighted materials or other intellectual property without authorization of the owner;
  4. Anything constituting or encouraging a criminal offense, giving rise to civil liability or otherwise violating any laws or our policies;
  5. Files that contain viruses, corrupted files, malicious code spyware or any other similar software or programs or any software in violation of copyright law or the applicable software license agreement;
  6. Advertising or promotional materials, including, without limitation, junk mail, surveys, spam, chain letters, pyramid schemes or other form of solicitation or unauthorized communication;
- (e) To engage in activities that result or may result in unauthorized billing or direct cost to the company;
- (f) To knowingly compromise the security of any portion of the network or use any of the networks in any manner or for any purpose not specifically authorized. This includes but is not limited to attempts to modify, “hack”, “scan”, “sniff” network traffic, probe hosts or disrupt the network in any manner;
- (g) To collect personal information about other users of the network, associates, customers, consultants, business partners whose information is stored or accessible on the network;
- (h) To modify, adapt, participate in the transfer or sale of, create derivative works from, distribute or reverse engineer any of the network, applications or data accessible through an associate connection, in whole or in part; take software written for LBI;
- (i) To impersonate another person or entity, engage in activities intended to withhold a user’s identity, or forge data with the intent to misrepresent the originating use or source;
- (j) To access Internet mail, web mail and/or personal e-mail accounts.
- (k) To allow non-associates (e.g. family or friends) to use LBI technology assets.
- (l) To post company material/video on Internet sites without the express permission of LBI management.

#### ***IV. Monitoring and Your Privacy***

Consistent with the approval process outlined below, LBI may, and likely will, at its discretion, monitor associate or contractor activity on the network and/or audit the use of its technology assets for any reason at any time without prior notice.

- Connection to and use of LBI network or technology assets constitutes consent to such monitoring and information disclosure.
- Individuals have no reasonable expectation of privacy while using any portion of the LBI network. As a result of LBI monitoring and/or audit process, personal activities carried out using LBI owned technology assets or network resources may become known to others.
- LBI assumes no responsibility or liability whatsoever for the protection of information or disclosure related to associate or contractor use of its resources or transfer of his or her data over its network.

To ensure adherence to and enforcement of this acceptable use policy, requests to review a current associate's or contractor's usage activity (e.g. e-mail, voice mail, Internet activity, instant messaging, blogs, phone records or online personal files/directories) must be presented to the office of the General Counsel for authorization. Authorization from the Office of the General Counsel is not required if the affected associate grants approval in writing for the requested access or information, or if the manager of a former associate requires access to the former associate's data for business purposes. In the case of the latter, the manager may have access for a period up to 30 days. Extended access requires authorization from the Office of the General Counsel.

#### ***V. Software Installation on LBI Computers***

No software may be installed on LBI computer systems unless the installation is performed in accordance with LTS technology standards and procedures.

The installation/use of unauthorized software has the potential to (1) impact the performance of equipment, (2) expose the company to a violation of copyright infringement laws and (3) introduce the spread of viruses, worms and spyware. Unauthorized software, documentation or data storage may be removed or blocked by the company at any time and without notification to the offending party.

- Installation/copying of software or storage of software, video files, music files and other data or documentation in a manner that violates a vendor license agreement, violates any copyright laws, or does not serve a legitimate business function is unauthorized and is prohibited.

#### ***VI. Certification of Your Equipment on LBI Network***

Connection of associate or contractor personal owned equipment to the company network is prohibited unless the standard service request form has been submitted and approved and there are reasonable operational or financial limitations preventing use of LBI provided equipment. This includes but is not limited to technology assets such as those listed in LBI ISP section "1.7.1 Electronic Equipment/Information and Communications". Contractor owned computing equipment must meet the following configuration requirements or it will be blocked from connecting to LBI networks:

- (a) Operating Systems: LTS authorized Operating Systems.
- (b) Service Packs: latest service packs recommended by the vendor for LTS authorized Operating Systems.
- (c) Critical Patches: all critical patches recommended by the vendor for LTS authorized Operating Systems.
- (d) Security Software: LTS authorized security software (Anti-Virus, Anti-Spyware, personal firewall/workstation intrusion detection system) must be active, properly configured and current.
- (e) Remote Access: must be provided by standard LTS authorized remote access systems.
- (f) LBI Inspection. Contractor must agree that authorized LTS associates can inspect their equipment for compliance to the terms and conditions of this Acceptable Use Policy. They must agree that no "lock-down" policy, i.e., "Group Policies" will be incorporated into the OS preventing LBI staff from confirming the installation of service packs, critical patches or virus definition files or which prevent the installation of same. During any period contractor equipment has a Connection to the LBI Network, LTS reserves the right to re-certify the equipment upon notice to contractor and without liability to contractor.

#### ***VII. Online Message Retention on LBI Email Systems***

Associates and Contractors must promptly delete messages sent or received that no longer require action or are not

necessary to ongoing projects. Electronic messages older than ninety days will automatically be deleted from mailboxes. Messages must not be moved or copied from the e-mail server in the form of message files or personal storage files (PST files). Exceptions to this policy require the express written authorization from General Counsel.

### ***VIII. Permitted Purposes and Content***

Your Connection is limited to Your internal use in the ordinary course of Your business only as You are authorized to establish that Connection solely for the purpose of fulfilling Your obligations with respect to LBI (the "Permitted Purpose"). You are permitted and authorized to maintain Your Connection only (a) so long as necessary to fulfill Your obligation, (b) Your equipment certification remains current, and (c) only for the Permitted Purpose.

Provided You maintain all copyright and other proprietary notices contained in any content, You may download and use content from the Network from any LBI-owned materials for the Permitted Purpose, but not for any other purpose. This limited authorization is non-transferable and non-exclusive, does not extend to third party content, and is for use only by You and Your employees and authorized agents and subcontractors, and only in accordance with fulfilling Your obligation within the scope of Your employment as an associate or under Your vendor agreement with LBI. In addition, except as expressly set forth in this AUP, You may not use, disclose, copy, store, reproduce or in any way exploit any portion of the Network during Your Connection or thereafter.

You agree to abide by all applicable laws and regulations in Your use of the Network and comply with all laws regarding the export of technical data from the United States through the Network.

### ***IX. User IDs and Passwords***

If Your Connection and Permitted Purpose require a user ID and password, then each authorized user ("Users") must enter a valid User name and password ("Access Codes") to access the databases or access the Network's secure areas. Access Codes may not be disclosed to anyone not authorized to act on Your behalf. It is Your responsibility to safeguard and protect Your and Your employees' and authorized agents' and subcontractors' Access Codes and to monitor all use of these Access Codes for all purposes. You accept all responsibility for maintaining the security of Your and Your employees' and authorized agents' and subcontractors' Access Codes and for all utilization of the Network via such Access Codes, with or without Your knowledge or consent. You agree to notify LTS immediately if You or Your employees, authorized agents or subcontractors discover or suspect any unauthorized access or violation of security of LBI's Network or if You have lost or know of any loss of any of Your Access Codes or wish to terminate Your or a particular User's ID and Password or have such Access Codes changed.

### ***X. Termination of Your Connection***

LBI has the right, upon learning of actual or possible illegal or improper uses of Your Connection, or Your failure to fully conform to any of the terms and conditions of this AUP, to take action, as it deems necessary in its sole discretion, to stop the actual or suspected unauthorized use, including but not limited to, immediately and without notice to You, terminating Your Connection, deleting Your information and revoking Your authorization to use the Network. In addition, Your Connection will immediately terminate, without notice, if and when Your status as an authorized vendor under any signed vendor agreement terminates.

If at anytime You or LBI believe in good faith there has been a breach of security or misuse of information, or there is a serious risk of malicious code propagating and impacting the operations of the Network, Your equipment or other resources of Yours or LBI's, that party may immediately and without notice to the other suspend the Connection. However, the disconnecting party must advise the other in writing of the reason for such suspension within forty-eight (48) hours after suspension and the Connection may be reestablished once the other party has demonstrated the breach of security has been addressed and the risks have been mitigated.

Upon termination of Your right to establish a Connection granted hereunder, You agree that You will immediately and completely terminate Your Connection and cease using all data accessed through or on the Network.

### ***XI. Disclaimer of Warranties***

THE NETWORK IS PROVIDED "AS IS" AND "AS AVAILABLE". LBI MAKES NO WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, REGARDING THE NETWORK, THE DATA OR CONTENT LOCATED ON OR ACCESSED BY MEANS OF THE NETWORK, INCLUDING BUT NOT LIMITED TO MERCHANTABILITY, FITNESS FOR A PARTICULAR USE OR PURPOSE, TITLE, NON-INFRINGEMENT, DATABASE ACCURACY OR THE ABSENCE OF ANY ERRORS, INTERRUPTIONS OR OMISSIONS. LBI ALSO DISCLAIMS ANY RESPONSIBILITY FOR ANY DAMAGES YOU MAY SUFFER

BY CONNECTING TO LBI'S NETWORK, INCLUDING LOSS OF DATA, DELAYS, NONDELIVERIES OR MISDELIVERIES OF DATA, SERVICE INTERRUPTIONS OR DAMAGES DUE TO LBI'S ERRORS OR OMISSIONS. LBI ALSO DISCLAIMS ANY RESPONSIBILITY FOR ANY DAMAGES YOU MAY SUFFER BY INSTALLING OR CONFIGURING ANY SOFTWARE ON YOUR EQUIPMENT AS REQUIRED BY THIS AUP.

Additional disclaimers may be contained at various websites on the Network.

**END OF POLICY**