WHAT DOES IT MEAN TO ME?
Read this policy to understand what uses of L Brands information and technology assets are acceptable and what are not.

POLICY

L Brands information and technology assets must be used in accordance with L Brands policies and standards and not in a manner that adversely affects L Brands or others. L Brands has the right to monitor activities.

STANDARDS

2.1 Acceptable Use Standards

2.1.1 LBI is committed to enhancing the ability of individuals to perform their duties and increase their productivity through the use of technology assets.

2.1.2 Careless, inappropriate or unethical use of technology assets can have unintended consequences.

2.1.3 Individuals must use discretion and judgment consistent with LBI values when using technology assets.

2.1.4 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.

2.1.5 Violations may result in appropriate disciplinary action, up to and including termination of employment or contracted services, recovery of damages, legal action, filing of criminal charges and termination of access and recovery of technology assets or network resources.

2.1.6 Individuals who become aware of a potential violation of the acceptable use policy are encouraged to notify the LBI IT Help Desk (e.g. Associate Technology Services (ATS), IT Service Desk) so that formal incident response procedures can be initiated.

2.1.7 Store associates should notify their immediate supervisor or Security (e.g. Emergency Operations Center (EOC).)

2.1.8 Call center associates should notify their immediate supervisor.

2.1.9 Exceptions to the acceptable use policy require business justification and will be reviewed by General Counsel and ISO.

2.1.10 Exception requests will expire one year from approval and requests must be submitted via the policy exception option within the SRF system available on GettingToNext.com.

2.2 L Brands Electronic Equipment/Information and Communications

2.2.1 LBI may provide individuals 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.

2.2.2 Technology assets include but are not limited to:

- **A.** Blogs (hosted on LBI' domains); Company social media websites
- **B.** Instant messaging
- **C.** Cloud Storage Solutions
- **D.** Network access, network resources, network devices (e.g. switches, hubs) and wireless networks
- **E.** Electronic mail (e-mail) includes but is not limited to Outlook/Exchange email and Aces Workmail
- **F.** Fax machines, telephones and voice mail
- **G.** Computer servers, workstations, and printers
- **H.** Internet access connectivity; Remote access connectivity
- **I.** Mobile devices such as laptops, tablets, smartphones, mobile POS, RF guns.
- **J.** Removable storage devices such as disk drives, tapes, USB drives, CD/DVDs.

2.2.3 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 personal securities or banking transactions;
- **D.** To knowingly use or spread (i.e., access, download, upload, transmit) the following material:
  - **a.** Material that violates the Company's Code of Conduct or policies — for example, material that contains derogatory racial or gender-related comments, pornographic or obscene materials or derogatory religious comments;

b. Information that is knowingly, recklessly or maliciously false;
c. Anything that is illegal;
d. 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;
e. Solicitations of any kind, including without limitation mass email, junk mail, surveys, spam, chain letters, pyramid schemes or other forms of unauthorized communication or any other forms of communication in violation of LBI Solicitation & Distribution policy.

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", or "sniff" network traffic, probe hosts or disrupt the network in any manner;
G. To collect, access, use or distribute personal information about associates, customers, consultants or business partners whose information is stored or accessible on the network, unless authorized to do so;
H. To share password login information with any other person or entity, use other individuals' account names or passwords or attempt to access resources to which the Associate has not been given authorized access;
I. To modify, adapt, create derivative works from or participate in the transfer, distribution or sale of any elements of the Network, applications or data accessible through your connection;
J. 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;
K. To access personal instant messaging accounts or forward company email to personal email accounts.
L. To allow non-associate personal contacts (e.g. family or friends) to use LBI technology assets.
M. To provide LBI e-mail addresses unless required for business purposes.
N. To post Company information or video, including logos and trademarks on any Internet sites without the express written permission of LBI management.
O. To download or install software on LBI computer systems unless the installation is authorized by LBI IT and performed in accordance with LBI IT technology standards and procedures.
P. To download, install, use, copy, transmit or store video files, music files, intellectual property, copyrighted material and other data or documentation in a manner that violates an external party license agreement, violates any copyright laws, or does not serve a legitimate business function.
Q. To retain credit card, social security or bank account numbers on a desktop/laptop or mobile device.
R. To download or copy company information onto non LBI-approved removable storage devices (e.g. disk drives, tapes, USB drives, CD/DVDs). Any removable storage device connecting to LBI assets must be encrypted and provided by LBI. [1]
S. To download or copy company information onto non LBI-Approved cloud storage solutions [2]

2.3 Monitoring

2.3.1 LBI respects your privacy. However, individuals have no expectation of privacy related to their use of LBI's assets and networks.
2.3.2 LBI may monitor and inspect its assets when LBI believes it is appropriate or necessary to further our business, and to protect our customers and you.
2.3.3 These assets include the communications and computing devices, services, and applications that we provide to associates and contractors (collectively, the "Network").
2.3.4 Accordingly, LBI may intercept; access; collect; use; and move, communicate, or transfer (including across borders) any information that is communicated by or through, or which is stored on, the Network.
2.3.5 These rights apply wherever that information may be located, such as laptop computers and peripheral devices.
2.3.6 Your connection to and use of the Network constitutes your consent for LBI to intercept; access; collect; use; and move, communicate, or transfer (including across borders) such information.
2.3.7 As a result of the LBI's activities, your personal activities carried out using LBI-owned technology assets or Network resources may become known to others.
2.3.8 LBI assumes no responsibility or liability whatsoever for the protection of information or disclosure related to your use of LBI's assets or your transfer of data over its Network.
2.3.9 Any request to intercept; access; collect; use; and move, communicate, or transfer (including across borders) a current associate's or contractor's communications and data activity must be presented to the Office of the General Counsel for authorization.

2.3.10 Authorization from the Office of the General Counsel is not required if the manager of a former associate or contractor requires access to the former associate's or contractor's stored 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.

2.3.11 Unauthorized software, documentation, data storage and technology assets may be removed or blocked by LBI at any time and without notification to the offending party. LBI proactively blocks access to inappropriate websites.

2.4 Network Access Standards

2.4.1 Devices must be authorized before being allowed access to L Brands' networks. (Reference the chart below for details.)

	Wired Networks	Wireless Networks	Remote Access
A. L Brands-Issued Devices			
1. Networks and Network Services Accessibility	a. May access wired networks with access to L Brands network services	b. May access corporate wireless networks with access to L Brands network resources. c. May not access L Brands public wireless networks.	d. May remotely access the network with access to L Brands network resources
2. Means of Access	a. Direct plug-in	b. Corporate SSID	c. VPN, per-application VPN via MDM, or VDI
3. Authentication	a. User authentication and device authentication	b. User authentication and device authentication	c. Based on means of access: i. VDI: user authentication with MFA ii. VPN: user authentication with MFA iii. Per-application VPN via MDM: user authentication
B. Associate Choice Devices			
1. Networks and Network Services Accessibility	*Not Applicable*	a. May access corporate wireless networks with access to public internet services only b. May not access L Brands public wireless networks	c. May remotely access network with access to L Brands network services
2. Means of Access	*Not Applicable*	a. Corporate SSID	b. Per-application VPN via MDM, or VDI
3. Authentication	*Not Applicable*	a. User authentication and device authentication	b. Based on means of access: i. Per application VPN via MDM: user authentication ii. VDI: user authentication with MFA
C. Associate and Vendor Personal Devices			
1. Networks and Network Services Accessibility	*Not Applicable*	a. May not access corporate wireless networks b. May access public wireless networks with access to public internet services only	c. May remotely access remote network with access to L Brands network services
2. Means of Access	*Not Applicable*	a. Public SSID	b. VDI
3. Authentication	*Not Applicable*	a. User authentication and device authentication	b. User authentication with MFA

2.4.2 Authorization Procedures

A. Users shall have direct access only to the networks and network services that they have been specifically authorized to use.

B. Access to all networks (except public wireless) and network services (except public internet services) must be authorized through the Request Management (Service Request Form (SRF)) process.

C. Access to corporate wireless networks in locations with neighboring buildings must be authorized every 24 hours through a registration process dictated based upon user type:

a. Associates must self-register

b. Vendors must be registered by an associate sponsor

2.4.3 Management Controls and Procedures

A. Network access controls and procedures must be maintained to protect access to network connections and network services.

2.4.4 Remote Access

A. Remote access service via LBI systems is provided for legitimate business reasons and activities on the LBI remote access system are governed by the acceptable use policy.

B. Standard LBI IT remote access packages must be utilized for all remote connectivity to the LBI network. LBI IT will not configure remote access connectivity or troubleshoot remote access with unauthorized third parties.

C. All devices connecting remotely to the LBI network must be authorized and must be running active, properly configured and current LBI standard security software as defined by LBI IT and LBI ISP.

D. Remote access connectivity must be disconnected if connection session is inactive.

E. Remote access connectivity to the LBI network must be provided via encrypted sessions (e.g. SSL, VPN). Encryption standards must follow those defined in LBI ISP.

F. Split tunneling must be disabled in remote access to prevent traffic from passing between the remote computer, the user's local network and the LBI network.

G. Multi-factor authentication must be in place for end-user full network remote access.

2.5 Online Message Retention on L Brands E-mail Systems

2.5.1 Associates must promptly delete messages sent or received that no longer require action, are not necessary to ongoing projects or are not relevant to any litigation record hold notices.

2.5.2 Absent prior written approval from the Office of the General Counsel, electronic messages older than 365 days will automatically be deleted from mailboxes and PST files are prohibited.

2.5.3 Associates must consider and adhere to data classification and handling standards as defined in the information security policies.

[1] *To obtain an **LBI-approved** encrypted removable storage device, submit a service request.*
[2] *To obtain access to an **LBI-approved** cloud storage solution, submit a service request.*

REVISION HISTORY

Revision	Date of Revision	Responsible	Summary of Revision
4.0	2016-10-03	Michelle Hutchison	2016 Information Security Policy Assessment
4.0	2018-11-31	Barbara Malone	Update policy statement 2.5.2 for email retention from 90 days to 365 days
4.1	2019-07-25	Barbara Malone Kim Jenkins	Update policy statements for use of removable storage devices and cloud storage solutions
4.1	2020-02-04	Barbara Malone	• Change made in 2018-11-31 was reverted back to 90 days when 2019-07-25 updates were implemented. This revision is to update 2.5.2 email retention to state 365 days. • Updated company logo.