Internet Usage Policy – Enterprise IT

Document Version / Details: Ver. 1.0/ 21st Feb 2024

Record of Release:

Version No.	Modified By	Reviewed By	Authorized By	Release Date	Modification Done
1.0	Sanjeev Kumar Jamadar	Ravindra Balekai	Ramesh T Kumar	21st Feb 2024	This document is derived from Mindtree document Internet Usage Document Ver.3.9 on 13-jan-2022.

Table of Contents

Purpose of this document

This document provides specific instructions on the ways to secure Internet usage and the policies related to the internet usage by LTIMindtree Minds.

Scope of this document

The policies apply to LTIMindtree users, contractors, consultants, temporary users, and others accessing internet resources in LTIMindtree Network and covers Internet usage on LTIMindtree desktops, laptops, and servers if these systems are under the jurisdiction and/or ownership of LTIMindtree. The policy also applies to stand-alone personal computers with broadband connections that are attached to LTIMindtree network.

Definitions, Abbreviation and Acronyms

The terms in use in the document are explained below:

Acronym	Description
EIT	Enterprise IT
SAM	Software Asset Management
ZIA	Zscaler internet Access
ZPA	Zscaler Private Access
ZCC	Zscaler Client Connector
ZDX	Zscaler Digital Experience

1 Introduction

The purpose of this policy is to establish procedures to ensure appropriate protection of LTIMindtree's information and equipment(s) by safe and secure Internet connection.
Throughout this policy, the word "users" will be used to collectively refer to LTIMindtree users, contractors, consultants, temporary users, and any other users who access the Internet from LTIMindtree network – either through the proxy or from the dial up modems/broadband connections or from any other means of Internet connectivity provided my LTIMindtree.

All Internet users are expected to be familiar with and comply with these policies. Any queries in this regard should be directed to the EIT Network team. Violations of these policies can lead to revocation of system privileges and/or disciplinary action, including termination.

Zscaler Internet Access is enabled for Web content filtering and to block malicious traffic including Zero days. Traditional proxies only inspect port 80 and 443 traffic. But we have subscribed to Zscaler Next Generation Firewall (NGFW) to monitor and block not only 80 and 443 but other ports and protocols as well. NGFW performs deep packet inspection and prevents intrusions to safeguard LTIMindtree assets. Zscaler Digital Experience (ZDX) capabilities are enabled to trace the packet drops and to fix any issues arising over the internet channels.

2 Overview

All information travelling over LTIMindtree networks is considered as LTIMindtree assets. It is the policy of LTIMindtree to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy of LTIMindtree to protect information belonging to third parties entrusted to LTIMindtree in confidence as well as in accordance with applicable contracts and SLA.

All LAN & Home users shall be able to access Internet through Zscaler which is managed by Enterprise IT.

- Zscaler shall be enabled for authentication. This means, only authorized domain users with valid credentials can access the Internet.
- Zscaler client forwards all Internet traffic to Zscaler cloud which filter the URL of websites and shall have capabilities to scan Virus at Gateway.
- User behavior on the Internet will be monitored and recorded. Usage data shall be stored for 180 days. After 180 days, the data shall be removed from the system.
- The report on usage can be submitted to management on request or as required.
- In case, Project Manager / Member of leadership team wish to seek detailed report, EIT Network can be contacted.
- Zscaler Client Connector (ZCC) will be disabled when the users connect to customer provided VPN or proxy. The same will be automatically enabled upon disconnections from customer VPN.
- Defined access polices (referenced under section 5) are applicable to all competencies and few users have elevated access privileges for business requirements. Please refer to the table under 'Web browsing categories' and the status of accesses.
- The tool intercepts SSL traffic for all URL categories with the exception to banking sites and business requirements.

2.1 Categories explicitly blocked for all users.

- AI and ML Applications, DNS over HTTPS, FileHost, Image Host, Shareware Download, Web Host, Online Chat, Peer-to-Peer Site, Remote Access Tools, Adult Sex Education, Adult Themes, Body Art, K-12 Sex Education, Lingerie/Bikini, Nudity, Other Adult Material, Pornography, Social Networking Adult, Marijuana, Other Drugs, Gambling, Anonymizer, Computer Hacking, Copyright Infringement, Mature Humor, Other Illegal or Questionable, Profanity, Questionable, Militancy/Hate and Extremism, Tasteless, Violence, Weapons/Bombs, Online and Other Games, Social Networking Games, Alt/New Age, Cult, Other Religion, Traditional Religion, Family Issues, Other Social and Family Issues, Social Issues, Alcohol/Tobacco, Special Interests/Social Organizations, Custom Encrypted Content, Dynamic DNS Host, Other Security, Spyware/Adware
- Categories that are blocked as a standard LTIMindtree policy can be access enabled as an exception post receiving approval from the CIO/CISO's and the request shall be business justified.
- Access to web-based mail has been allowed as read only. Sending attachments are blocked while the users can download the attachments.

- Downloading executables are blocked.
- Uploading files to public sites are prohibited with an exception to business requirements.
- Access to certain public Instant messaging / customer provided tools are allowed purely for business use as users need to chat with onsite users or clients at remote locations. Users shall shut down the IM client when not in use. Users shall use this only for business. Voice and video over IM are not allowed.
- Github & Filesharing sites are blocked for users who are serving notice period.

For further details please refer to the section "Web Browsing categories and status of access"

2.2 Users Responsibilities

Because of the wide-open and unregulated nature of the Internet, misuse of Internet access could have severe adverse consequence for LTIMindtree. This section establishes usage rules for all Users.

2.2.1 Illegal and/or Inappropriate Usage

- Software without an appropriate licensing agreement must not be downloaded or copied from the Internet. Agreeing to the terms of any "clickwrap", "browse wrap", or other online agreement on behalf of LTIMindtree is not permitted without prior approval from Legal and, as applicable, the Business head as well.
- Knowingly or negligently injecting viruses into any system, transmitting materials damaging to the files or programs or engaging in any other form of cracking is strictly prohibited.
- Accessing or transmission of offensive, obscene, and harassing material is prohibited.
- Material that violates any applicable international, national, or local law or regulation must not be transmitted using LTIMindtree Network.
- It is inappropriate to deliberately or negligently perform any act that will impair the operation of any part of the LTIMindtree corporate network or deny access by legitimate users of the LTIMindtree Internet application systems. This includes, but is not limited to, knowingly wasting resources, tampering with components, or deliberately reducing the operational efficiency of LTIMindtree corporate network.
- Under no circumstances users can utilize the LTIMindtree corporate network and system for personal gain. LTIMindtree reserves the right to investigate and prosecute users. (Read limited personal use below)
- LTIMindtree sensitive and confidential information must never be sent over the Internet unless it has first been encrypted by approved encryption methods.

2.2.2 Downloads and File Transfer Controls

- Commercial software must be obtained only through appropriate procurement channels.
- Users shall not copy LTIMindtree provided software to public network or take it to home. Any home use of LTIMindtree software must be approved and documented by SAM Team. However, LTIMindtree has home use right of Microsoft Office as per details available on LTIMindtree Intranet.

- Machine-readable software and data files must be obtained only from reliable and trusted sources or sites.
- Shareware and freeware software must not be installed without explicit approval from the client or/and Enterprise IT Head for project use.
- All newly acquired software, regardless of the source, must be scanned using procedures established by the Virus Protection Policy and standard. It is important to note that viruses are normally introduced into a system by a voluntary act of a user (e.g., installation of an application, FTP of a file, reading mail, etc.). Computer viruses are often spread through free or shared programs, games, demonstration programs, and programs downloaded from bulletin boards. However, it must be noted that the worms of last few years have changed things where most Malicious Software is spread via Internet access.
- Users shall not download songs / movies / games.
- Online gaming is prohibited.
- Every user is provided with unlimited internet access throughout the day to perform business-related activities.
- Open-Source Downloads are blocked from Zscaler; however, the request can be forwarded to Software Asset Management (SAM) team or open an iSupport ticket to have the SAM team assist you.
- File Control Downloads are Blocked from Zscaler, Like Executables, Audio/Video, Archive files, Mobile & Online Gaming.
- Few Exceptions like Downloads of office Documents, PDF, Images, Active web Contents are allowed from Proxy.

2.2.3 Public Representations

- Users must not publicly disclose internal LTIMindtree information via the Internet channels unless the approval Security team is obtained.
- Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, social media and related public postings on the Internet. If a user is working on an unannounced product, a research and development project, or related confidential matters, all related postings must be cleared by the one's Project Manager and/ or Delivery Heads prior to being placed in a public spot on the Internet.

2.2.4 Resource Usage for limited personal use

- Use of computing resources for limited personal purposes (like viewing Bank account / use for booking train / airline tickets / News website / financial information) is permissible so long as the incremental cost of the usage is negligible, and so long as no business activity is pre-empted by the personal use. Extended use of these resources requires prior written approval of the reporting manager.

2.2.5 Information Movement

- All downloads from non LTIMindtree Network sources via the Internet must be screened with virus detection software before being opened or run. Whenever the provider of the software is not trusted, the downloaded software must be installed on a stand-alone (not connected to the network) non-production machine. If this

software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

- All information fetched from the Internet should be considered suspect until confirmed by reliable sources. There is no quality control process on the Internet, and a considerable amount of its information could be either outdated or inaccurate.
- It is also relatively easy to spoof another user on the Internet. Likewise, contacts made over the Internet should not be trusted with LTIMindtree information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal LTIMindtree information.
  Users must not place LTIMindtree's material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP) or similar services, unless the Head of Marketing or the Business President has first approved the posting of these materials.
- All publicly downloadable (common/public) directories on LTIMindtree's Internet-connected systems should be reviewed and cleared periodically. This process is necessary to prevent the anonymous exchange of information inconsistent with LTIMindtree's business.

2.2.6 Information Protection

- Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, LTIMindtree's secret, proprietary, or private information must not be sent over the Internet.
- Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.
- Credit card numbers, telephone calling card numbers, log in passwords, and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form.
- In keeping with the confidentiality agreements signed by all users, LTIMindtree's software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-LTIMindtree party for any purposes other than business purposes expressly authorized by management.
- Exchanges of software and/or data between LTIMindtree and any third party should not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.
- Regular business practices—such as shipment of software in response to a customer purchase order—need not involve such a specific agreement since the terms are implied.
- LTIMindtree strongly supports strict adherence to software vendors' license agreements. When at work, or when LTIMindtree computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.
- Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with LTIMindtree work and are therefore prohibited. Similarly, reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner.

2.2.7 Expectation of Privacy

- Users using LTIMindtree information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. At any time and without prior notice, management reserves the right to examine e-mail, personal file directories, and other information stored on computers. This examination assures compliance with internal policies, supports the performance of internal investigations.

2.2.8 Resource Usage

- LTIMindtree Network encourages users to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not company, resources. Likewise, games, news groups, and other non-business activities must be performed on personal resources and during personal time.
- Use of computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no business activity is pre-empted by personal use. Extended use of these resources requires prior written approval of the reporting manager.
- Based on the usage pattern and status of Bandwidth, LTIMindtree can implement web filtering of certain sites. Such list will be published on Ultimaworks and will be updated on regular basis.

3 Tips for Safe Web browsing

- Please exercise extreme caution while browsing websites on the internet. Watch out for any suspicious activity that may happen as part of your browsing. Stay away deliberately from any questionable sites, including pornography, gambling, hacking, or other off-beat sites. (e.g.: Do not venture out on opening by clicking websites which looks strange or are unheard). Never install or run any plug-ins or active contents like ActiveX, Applets from un-trusted sources. Ensure web browser security settings are high or set to disallow unsigned ActiveX and components.
- Pop-up Window Closure: Please refrain from clicking the “Agree” or “OK” buttons that you may find in any of suspicious pop-up windows. These buttons can masquerade as innocent features that inadvertently start an unwanted download of Spyware/adware program. Instead, close the window. Ideally the web browser setting to block pop-ups should be enabled.
- Freeware downloads: Never deliberately download freeware/shareware utilities, Chrome Extensions and Firefox plugins to your desktop/laptop from the Internet, no matter how helpful or interesting it may appear. This could even include various types of anti-spyware software as well. Even innocuous toolbars and nifty utilities can be packed with unwanted piece of software (spyware/adware programs).
- File Sharing: If connected to internet from public places, please refrain from sharing any directory/files in your laptop without privilege control.

4 Inspection and Malware analysis

Tool should be capable to analyze the modern-day threats and block them at the gateway. With regards to this, the below policy is applied at the gateway. We have

enabled Sandboxing capabilities that provides an additional layer of security against zero-day threats and Advanced Persistent Threats (APTs) through Sandbox analysis.

MALWARE POLICY	
TRAFFIC INSPECTION	
Inspect Inbound Traffic	Yes
Inspect Outbound Traffic	Yes
PROTOCOL INSPECTION	
Inspect HTTP	Yes
Inspect FTP over HTTP	Yes
Inspect FTP	Yes
MALWARE PROTECTION	
Viruses	Blocked
Unwanted Applications	Blocked
Trojans	Blocked
Worms	Blocked
Sandbox Ransomware	Blocked
ADWARE/SPYWARE PROTECTION	
Adware	Blocked
Spyware	Blocked
Password-Protected Files	Blocked
Unscannable Files	Blocked

Advanced Threat Protection	
BOTNET PROTECTION	
Command & Control Servers	Blocked
Command & Control Traffic	Blocked
Domain Generated Algorithm (DGA) domains	Enabled
MALICIOUS ACTIVE CONTENT PROTECTION	
Malicious Content & Sites	Blocked
Vulnerable ActiveX Controls	Blocked
Browser Exploits	Blocked
File Format Vulnerabilities	Blocked
FRAUD PROTECTION	
Known Phishing Sites	Blocked
Suspected Phishing Sites	Blocked
Spyware Callback	Blocked
Web Spam	Blocked
Crypto Mining	Blocked
Known Adware & Spyware Sites	Blocked

UNAUTHORIZED COMMUNICATION PROTECTION	
IRC Tunnelling	Blocked
SSH Tunnelling	Blocked
Anonymizers	Blocked
CROSS-SITE SCRIPTING (XSS) PROTECTION	
Cookie Stealing	Blocked
Potentially Malicious Requests	Blocked
P2P FILE SHARING PROTECTION	
BitTorrent	Blocked
P2P ANONYMIZER PROTECTION	
Tor	Blocked
P2P VOIP PROTECTION	
Google Hangouts	Blocked

5 Web browsing categories and the status of access

S.No.	Categories	LTIMindtree Network / Road Warrior
	Entertainment/Recreation	
1	Entertainment	Allowed
2	Music and Audio Streaming	Allowed
3	Other Entertainment/Recreation	Allowed
4	Radio Stations	Allowed
5	Video Streaming	Allowed
6	Television/Movies	Allowed
	News and Media	
7	News and Media	Allowed
	Business and Economy	
8	Classifieds	Allowed
9	Corporate Marketing	Allowed
10	Finance	Allowed
11	Online Trading, Brokerage, Insurance	Allowed
12	Other Business and Economy	Allowed
13	Professional Services	Allowed
	Education	
14	Continuing Education/Colleges	Allowed

15	History	Allowed
16	K-12	Allowed
17	Other Education	Allowed
18	Reference Sites	Allowed
19	Science/Tech	Allowed
	Information Technology	
20	Advertising	Allowed
21	AI and ML Applications	Blocked
22	CDN	Allowed
23	DNS over HTTPS	Blocked
24	FileHost	Blocked
25	Image Host	Blocked
26	Operating System and Software Updates	Allowed
27	Other Information Technology	Allowed
28	Portals	Allowed
29	Safe Search Engine	Allowed
30	Shareware Download	Blocked
31	Translators	Allowed
32	Web Host	Blocked
33	Web Search	Allowed
	Internet Communication	
34	Blogs	Allowed
35	Discussion Forums	Allowed
36	Internet Services	Allowed
37	Online Chat	Blocked
38	Other Internet Communication	Allowed
39	Peer-to-Peer Site	Blocked
40	Remote Access Tools	Blocked
41	Webmail	Allowed File Attachment Blocked
42	Web Conferencing	Allowed
43	Zscaler Proxy Ips	Allowed
	Job/Employment Search	
44	Job/Employment Search	Allowed
	Government and Politics	
45	Government	Allowed
46	Military	Allowed
47	Other Government and Politics	Allowed
48	Politics	Allowed

	Miscellaneous	
49	Miscellaneous or Unknown	Allowed on Browser Isolation
50	Newly Registered Domains	Allowed on Browser Isolation
51	Non Categorizable	Allowed on Browser Isolation
52	Other Miscellaneous	Allowed on Browser Isolation
	Travel	
53	Travel	Allowed
	Vehicles	
54	Vehicles	Allowed
	Adult Material	
55	Adult Sex Education	Blocked
56	Adult Themes	Blocked
	Body Art	Blocked
57	K-12 Sex Education	Blocked
58	Lingerie/Bikini	Blocked
59	Nudity	Blocked
60	Other Adult Material	Blocked
61	Pornography	Blocked
62	Social Networking Adult	Blocked
	Drugs	
63	Marijuana	Blocked
64	Other Drugs	Blocked
	Gambling	
65	Gambling	Blocked
	Illegal or Questionable	
66	Anonymizer	Blocked
67	Computer Hacking	Blocked
68	Copyright Infringement	Blocked
69	Mature Humor	Blocked
70	Other Illegal or Questionable	Blocked
71	Profanity	Blocked
72	Questionable	Blocked
	Militancy/Hate and Extremism	
73	Militancy/Hate and Extremism	Blocked

	Tasteless	
74	Tasteless	Blocked
	Violence	
75	Violence	Blocked
	Weapons/Bombs	
76	Weapons/Bombs	Blocked
	Games	
77	Online and Other Games	Blocked
78	Social Networking Games	Blocked
	Health	
79	Health	Allowed
	Religion	
80	Alt/New Age	Blocked
81	Cult	Blocked
82	Other Religion	Blocked
83	Traditional Religion	Blocked
	Shopping and Auctions	
84	Online Auctions	Allowed
85	Online Shopping	Allowed
86	Other Shopping and Auctions	Allowed
87	Real Estate	Allowed
	Social and Family Issues	
88	Family Issues	Blocked
89	Other Social and Family Issues	Blocked
90	Social Issues	Blocked
	Society and Lifestyle	
91	Alcohol/Tobacco	Blocked
92	Lifestyle	Allowed
93	Art/Culture	Allowed
94	Dining/Restaurant	Allowed
95	Hobbies/Leisure	Allowed
96	Other Society and Lifestyle	Allowed
97	Social Networking	Allowed File Upload & Posting Blocked

	Special Interests/Social Organizations	
98	Special Interests/Social Organizations	Blocked
	Sports	
99	Sports	Allowed
	Security	
100	Custom Encrypted Content	Blocked
101	Dynamic DNS Host	Blocked
	Newly Revived Domains	Blocked
102	Other Security	Blocked
103	Spyware/Adware	Blocked

6 Road-Warrior Policy

All Laptops must be installed with end point agent called ZCC. When users browse over broadband internet connections, the policy stated above will be applied. In conjunction, ZPA is part of ZCC client and is enabled for users based on VPN needs. For more information, please refer to LTIMindtree VPN policy.

7 Reporting Security Problems

In case of following security threats, please notify the Information Security Compliance team or Enterprise IT Team.

- If sensitive LTIMindtree Network information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties.
- If any unauthorized use of LTIMindtree's information systems has taken place, or is suspected of taking place.
- Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, Enterprise IT team should be notified immediately.
- Because it may indicate a computer virus infection or similar security problem, all unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported to Enterprise IT Team. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

8 Disciplinary Process

Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.

LTIMindtree

Let’s get to the future, faster. Together.