

The following policies are applicable to all staff, including permanent employees, people on contract, consultants, advisors, retainers, interns, trainees and all individuals working directly for IL&FS, unless otherwise specifically mentioned

I. **Service Code of Conduct** :

The purpose of this is to define a Service Code of Conduct for all staff of IL&FS. The Service Code of Conduct would be applicable to all staff immediately on their joining the Company, and all staff would be deemed to have read and understood the Service Code of Conduct on joining the Company

Any staff found breaching the Service Code of Conduct would be liable for disciplinary action by the appropriate authority, including termination of services, if so required

1. **Outside Business** : Each officer and the staff must obtain prior written approval of the Company with respect to outside business activities. Prior to engaging in such activities, an officer or the staff must obtain necessary approvals from the Competent Authority. Such approval, if granted, may be given subject to restrictions or qualifications and is revocable at any time. Examples of activities requiring prior written approval include full or part-time service as an officer, director, partner, consultant or staff of another business organisation (including acting as a director of a company whose securities are publicly traded); contributing (whether for payment or not) written articles in newspapers, magazines, journals of professional or trade 'bodies, etc.; agreements to provide financial advice to a

Private, educational or charitable organization, and any agreement to be employed by or accept compensation in any form (e.g. salary, fee, commission, bonus etc) from a person or entity other than the Company or its subsidiaries and affiliates

2. **Confidentiality** : All staff shall maintain the strictest confidentiality regarding the Company's affairs and the affairs of its constituents, and shall not divulge, directly or indirectly, any information either to a member of the public or of the Company's staff, unless compelled to do so by a judicial or other regulatory authority or unless instructed to do so by a superior officer in discharge of his duties. Any attendant liability that may arise out against the Company due to the breach of secrecy by the staff will be entirely to the staff's account

3. Compliance : All staff in discharging their duties, shall fully and promptly comply with all the applicable statutory and regulatory requirements, and if in doubt shall refer the matter to his supervisor and / or the competent authority for advice
4. Honesty & Integrity : All staff shall serve the Company honestly and faithfully and shall use his utmost endeavors to promote the interests of the Company and shall show courtesy and attention in all transactions and dealings with the Company's constituents
5. Media Contact : No staff shall, except with the prior sanction of the Competent Authority, own wholly or in part, or conduct or participate in the editing or management of any newspaper or any other periodical / publication. Further, no staff shall, except with the prior sanction of the Competent Authority or except in the bonafide discharge of his duties, participate in any radio broadcast or give any interview to a Programme telecast on Television, or contribute to any article or write any letter to any newspaper or periodical or make public or publish or cause to be published any documents, papers or information that shall relate to the business of the Company and which may have come into his possession in his official capacity. Any staff in breach of the above shall be held responsible for any loss or damage that may be caused to the Company
6. No staff shall, without the prior sanction of the Company, except in the discharge of his official duties, take part in the registration, promotion or management of a Company which is required to be registered under the Companies Act, 1956 (1 of 1956)
7. No staff shall bring or attempt to bring any political or other outside influence to bear upon any superior authority to further his interests in respect of matters pertaining to his services in the Company
8. In carrying out the business of the Company or in any matter involving the Company, no staff shall resort to bribing or offering any monetary benefit or in any way offering any favour other than in the normal course of business, to any official, government, regulatory or otherwise. No staff shall accept, seek, solicit, or accept, for his personal benefit, any gifts or presents in cash or of significant monetary value, for the professional services rendered or business deals done on behalf of the Company, from existing and / or prospective constituents.
9. Usage of Electronic / Internet facilities : The Company makes available various electronic facilities such as computer, printing, internet, etc. The use of these facilities by staff should be restricted solely to official purpose and for conducting the business of the Company. Any deviations of this in a manner other than described herein would require the approval of the Competent Authority

10. Abusive Substances : All staff shall refrain from subjecting themselves to any prohibited abusive substances such as narcotics and shall refrain from attending work and remaining in office premises while under the influence of any substance that impairs mental faculties (e.g. alcohol). As smoking is a potential health hazard for the smoker as well as the surrounding persons, no staff shall be permitted to smoke in the office premises other than in designated areas

11. Third Party Intellectual Rights : In the course of performance of their official duties, all staff will use or have access to Software, Databases and other materials in which third parties have copyright or other proprietary interest. These third party intellectual property rights shall be honored by the staff and the said materials shall not be copied (includes loading software or other material onto the hard drive of a computer, copying it onto a disk and any other transmission of material e.g., sending via e-mail) without obtaining the permission of the copyright owner. No staff should accept, solicit or seek rewards, compensation, gifts, or presents, of any significant monetary value, for his personal benefit, for the professional services rendered or business deals done on behalf of IL&FS, from existing and / or prospective constituents

12. Dress Code and Decorum : In order to project a professional business image of the Company and to maintain a sober and decorous working atmosphere, all staff shall be expected to adhere to a sober dress code. For normal working days, this will be formal wear and tie for gentlemen, and either saris, salwar suits or formal office wear for ladies. Staff are not permitted on working days to wear Jeans, T-shirts, or any clothing that is likely to affect the working environment adversely or convey an adverse image of the Company

The dress code on weekends and holidays may be casual, except when official meetings have been planned on such days. Further, given the 'open office' system being followed in most IL&FS offices, all staff are also urged to observe decorum at work and to desist from unnecessary and unseemingly loud and boisterous behavior

13. All staff shall fully comply with all applicable statutory/regulatory requirements and IL&FS's Corporate Policies and Procedures as mentioned in the above sections in respect of his department activities. In case of doubt, he should approach his supervisor for necessary guidance

14. Without prejudice to the provisions of the other Rules, a staff who commits a breach of the Rules of the Company, or who displays negligence, inefficiency or indolence, or who knowingly does anything detrimental to the interests of the Company or in conflict with its instructions, or who commits a breach of discipline or is guilty of any act of misconduct, shall be liable to the following penalties :
 - (a) Reprimand
 - (b) Postponement or stoppage of increment or promotion
 - (c) Demotion to a lower post or grade or to a lower stage in his incremental scale
 - (d) Recovery of the whole or part of any pecuniary loss caused to the Company
 - (e) Discharge
 - (f) Dismissal

15. A staff may be placed under suspension by the officer empowered to pass such orders. During such suspension, he shall receive a subsistence allowance as per the applicable laws, to be adjusted against salary and benefits at the final disposal of the case

II IT POLICIES

A. IT SYSYEM USAGE POLICY

i. Introduction

The Organization provides IT Assets and Services to the Users to conduct their business operations and to enhance the efficiency and quality of the same. Misuse (either intentionally or not) of the IT Assets may have serious consequences which may include loss / unauthorized disclosure of critical information, loss of productivity / efficiency, adverse publicity and/or legal liabilities which may eventually lead to significant business losses for the Organization. It is thus important to protect these IT Assets from illegal or damaging actions by Users to avoid exposing the Organization to any legal, reputational or financial risks

ii. Objective

The objective of this policy is to govern the usage, storage and handling of IT Assets and information that is contained in these IT Assets

iii. Responsibilities

1. All Users shall adhere to the guidelines regarding usage of PCs and Mobile Devices
2. IT Department :
 - a. Domain Specific Administrators shall be responsible for assisting the User from complying with the usage guidelines stated below
 - b. IT Domain Specific Managers shall be responsible for supervising the Domain Specific Administrators
3. Head of Departments shall be responsible for approving requests of the User with regard to usage of PCs and Mobile Devices

4. Policy Statements

(a) **General Policy**

- i. Any electronic data created, modified, altered and/or transmitted using any of the IT Assets or Services of the Organization shall be the sole property of the Organization and the User shall not claim otherwise
- ii. All usage of the IT Assets and/or Services shall be guided by the relevant IT Policies. The IT Assets and/or Services shall be primarily used for business purposes and may be used for reasonable personal use.

(b) **PC (Desktop / Laptop) Usage**

- i. This shall be applicable to the computer systems (including a desktop or laptop) provided by the Organization for business use (“PC”)
- ii. All Users shall:
 - Be responsible for the security of their PC and should take adequate measures to restrict physical and logical access to their PC.
 - Not change any hardware configuration, settings in operating system of the PC or any applications installed on their PC
 - Not install any software or applications on their PC unless on a request to the IT department
 - Request the IT department for any change in hardware configuration, software settings or additional software
 - Ensure only authorized software is installed on the PC of the user.

- Not download and/or store games, music or movie files in the PC
- Not to exchange/transfer of PC or any other IT equipment between Users or between organisations or across locations without seeking due approvals (including from IT Department).
- Ensure backup of their critical official data even though the data on the shared drive is backed up on the servers
- Use file servers for sharing files between multiple Users
- To prevent the risk of unauthorized access, ensure that:
 - The PCs are locked, if left unattended.
 - Standard screensaver and wall paper (approved by IT Department) shall be used.
 - Not enable sharing of folders with other Users which may lead to virus proliferation if the host computer is infected by a virus
- Take following precautions pertaining to the security of PCs:
 - Back up critical data regularly, especially before travelling with their laptop computers.
 - Not boot the PC from a removable media/device, to avoid the same being infected with virus/ malware
- Not change the display settings or IP addresses/subnets of the PC as has been set by the IT Department
- Not disclose the IP addressing scheme of the Organization to any third person

- Not use personal PCs on the network provided by the Organization
- Ensure that PC screens be kept clear of sensitive information when unattended

iii. To assist the User in complying with the above, the IT Department shall :

- Ensure all PCs be added in the central / regional domain of the Organization
- Ensure that critical system patches and updates for the PCs must be updated through central server
- At the request of any User and after receipt of due approvals, install such software after verification of the software to be installed, for license and security compliance
- Assist Users (in accordance with standard procedures) who have requested for any change in hardware configuration, software settings or additional software
- Remove/ uninstall any unauthorized / unlicensed software as and when the same is observed in any User's PC
- After receipt of due approvals, exchange/transfer PC or any other IT Assets between Users or between organisations or across locations in accordance with the standard procedure
- Ensure that PCs automatically lock after five minutes of inactivity.
- Provide any and all assistance to the User as maybe required from time to time
- Follow up with User/ facilitate Users to take backup of official data including corporate email systems like Lotus Notes

(c) **Mobile Device (Tablet/Smart Phones etc.) Usage**

- i. This shall be applicable to all Users using a tablet/ smartphone having corporate email access (“**Mobile Device**”)
- ii. Users shall :
 - Not be allowed to connect their personal mobile devices to the network of the Organization unless the same is checked and certified to be safe by IT Department
 - Be responsible for the security of information contained in such Mobile Devices
 - Secure the Mobile Devices using adequate password protection as stated in the IT Policies
 - Install anti-virus software with latest signatures on the Mobile Devices
 - Ensure that the Mobile Devices are periodically updated with all necessary security patches/ hot fixes for the operating system and applications installed on them.
 - Ensure that their Mobile Devices are backed up at regular intervals.
 - Take adequate measures for the physical protection of Mobile Devices including not leaving the same unattended in public places or while traveling.
 - Immediately report the loss of the Mobile Devices to the IT Department (along with any other specific information as maybe required by them) to prevent misuse of data
- iii. IT Department shall assist the User in achieving the aforesaid and provide timely support/ follow up with the Users on the same

5. Definitions of common terms used

- (a) Patch: An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
- (b) Screensaver: Software program which executes when a computing device is in idle state
- (c) Wallpaper: Image displayed on the desktop for personalization of a computing device

B. INTERNET USAGE POLICY

1. Introduction

Internet is a very powerful information resource. Proper use of the internet can enhance the capabilities of the User and the Organization. Access to the internet is a job necessity and helps in job enrichment by providing access to relevant resources at the click of a button. Since Internet is unregulated and uncensored, there are serious internet based risks which can paralyze the IT System of the Organization and result in loss or corruption of data and may also lead to statutory/regulatory implications. It is therefore necessary to set guidelines putting down appropriate internet usage restrictions upon the Users

2. Objective

The objective of this policy is to define the acceptable and unacceptable usage of the internet by Users

3. Responsibilities

- (a) Users are responsible for adherence to the policy guidelines and reporting violation or misuse
- (b) IT Security Administrators shall be responsible for managing compliance to this policy

- (c) IT Domain Specific Administrators must comply with this policy, follow its guidelines, and adhere to the same, for all systems configuration and settings
- (d) IT Domain Specific Managers are responsible for supervising the IT administrators towards adherence to the policy

4. Policy Statements

(a) **General Policy**

- i. Usage of internet help in enhancing the performance of the staff in the following ways:
 - Enhancement of Job :

Persons given internet access are expected to use the internet to enhance the performance of their work responsibilities. The data and information available on the internet can provide invaluable assistance with certain job-related tasks.
 - Enhancement of Organization :

Beneficial uses might include research data, the discovery of work-related information, white papers, the downloading licensed product updates, or the use of special online services and features
 - Enhancement of Skills :

Persons are encouraged to use the resources on the internet to enhance existing job-related skills.
- ii. Use for Official Business : The internet access is provided to Users as a business tool at significant cost. The facilities to provide internet access represents a considerable commitment of company resources for telecommunications, networking, software, storage, etc. Use of the internet by the Users should therefore be limited to

official and business purposes. Occasional and reasonable personal use of internet services may be permitted, provided however that such use is not for illegal or immoral purposes and does not interfere with work performance.

iii. Internet Access provided by the Organization :

- Users should access the internet only through the connectivity mediums (like wifi and LAN) provided by the Organization and should not set up any other internet access (like mobile access point or tethering from a mobile internet connection) without prior authorization from the IT Department
- All usage of internet services by the User should be in compliance with applicable Laws (including any rules, regulations and guidelines of the IT Act, SEBI guidelines or any statutory or regulatory compliance related to the Organization)
- The IT Department may restrict access to certain websites on the internet which affect the network performance of the Organization or are unethical or deemed malicious for the Organization at their sole discretion
- Notwithstanding the above, the Organization shall in its own discretion filter and/or prohibit access to certain websites
- Online conduct of the Users must reflect the ethics, professionalism, courtesy, and responsibility as expected by the Organization since the Users (while using the internet access provided by the Organizations) are acting as agents of the Organization
- Unauthorized or inappropriate use of the internet services by any User must be reported by users immediately to the IT Department

- Detection of external efforts to compromise the Organization's system security (for example by hackers) shall be reported immediately by any Users to the IT Department

(b) Responsibilities

i. All Users shall not:

- Download or distribute malicious software or tools or do anything similar activity to deliberately propagate any malware
- Stream and/or download media or video files or transfer bulky files (since this represent significant data traffic) which may cause network congestion. If any of the above is required by the User, it shall be done by the IT department
- Violate any copyright or license agreement by downloading and/or distributing copyright protected material or software available on the internet
- Upload files, software or data belonging to the Organization to any internet site or cloud software like Dropbox, Google Drive, OneDrive, etc. without prior authorization. Use only Secure File Transfer facilities provided by the IT Department in order to transfer bulky files
- Share any confidential and/or sensitive information of the Organization on or with any third person on any internet website unless the same is for official purposes which has been duly authorized
- Post any views and/or opinion on behalf of the Organization unless duly authorized
- Post remarks that are defamatory, racial, obscene or not in line with the Organization's policy
- Access obscene or explicit material available on the internet either directly or indirectly

- Conduct illegal or unethical activities including gambling or misrepresenting the Organization
 - Conduct in any online stock trading activities for personal benefit
 - Solicit money from any person or for advocating a religious or political cause from any persons via the internet
 - Use the Organization's Services including internet services, resources or facilities for any purposes that violate applicable Laws
 - Conduct activities which may compromise network security including without limitation disclosure of any system ids, passwords, and/or information that may allow the circumnavigation of security features of the IT Systems of the Organization.
 - Tamper, disable or circumvent any security system implemented in the IT Systems by the Organization to ensure the safety and security of the same
 - Use devices with their own internet data cards / Wi-Fi connection sharing, thereby establishing independent internet sessions having the effect of sidestepping the Organization's security mechanisms. This may be used by an attacker to compromise the IT Systems. Users should isolate the PC from the Organization's network before establishing a third party hosted internet connection
 - Access any websites by clicking on links provide in emails or in other websites to prevent unauthorized access of any sensitive data (including financial information). Users should, if required, enter the URL manually instead of clicking on the provided link
- iv. To achieve the aforesaid, IT Department shall educate the Users regarding the systems in place to track violations and non-adherence to the IT Policies, if any

(c) **Internet Usage Monitoring**

The Organization shall:

- i. Have the right to access, monitor, record, review, store and audit internet usage of all Users to analyze usage patterns or assure system security
- ii. If required under Law or on the request of a governmental authority, disclose any information with regard to the internet usage of any User
- iii. Have the right to conduct any forensic analysis of any internet usage of any User or delegate the same to a third party as may be required by the Organization

5. Definitions

- (a) **Wi-Fi:** A mechanism to connect to a computer network wirelessly
- (b) **Hacker:** Unauthorized user who attempts to or gains access to an information system

C. **CORPORATE EMAIL POLICY**

1. Introduction

Corporate email system is an important communication service provided by the Organization to the Users for carrying out day to day business related tasks. Improper use of corporate email system by Users can lead to unauthorized information disclosure and could bring the Organization to disrepute

2. Objective

This document has been prepared to ensure that the corporate email system is used by the Users of the Organization in accordance with the accepted norms associated with the usage of mailing system in a corporate environment. Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer is admissible as evidence in a court of law and therefore it is imperative that the usage of corporate email system is in accordance with the IT Policies

3. Responsibilities

- (a) Users are responsible for adherence to the policy guidelines and reporting violation or misuse of E-Mail Systems
- (b) IT Domain Specific Administrators must comply with this policy, follow its guidelines, and adhere to the same
- (c) IT Domain Specific Managers are responsible for supervising the IT administrators towards adherence to the policy
- (d) Head of Departments and Human Resources Departments are responsible for approving user requests in relation to email related activities
- (e) Human Resource Department is responsible for requesting and validating creation, renaming, store & forward and deletion of E-Mail IDs

4. Policy Statements

a. **Usage Policy**

All Users shall :

- i. Use the corporate email system for official and business use only. Occasional and reasonable use of corporate email system for personal purposes is allowed
- ii. Treat email messages and files as confidential information
- iii. Not use corporate mail system in any way which is disruptive, offensive to others, or harmful to morale
- iv. Not transfer or transmit sexually explicit images, messages, and cartoons or any ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others
- v. Use corporate email system as a business communication tool (which is admissible as evidence in a court of law) and use the same in a responsible, effective and lawful manner



- vi. Not use the corporate email system to solicit third persons for commercial ventures, religious or political causes, outside organizations, or other non-business matters
- vii. Not use their official email ID while subscribing or signing up for services like Facebook, Twitter, any such 3rd party service
- viii. Immediately report any suspected spurious emails to the IT Department since emails can carry viruses and/or other security risks
- ix. Not use corporate email IDs as the secondary email ID for any third party email systems
- x. Not forward any email from the Organization's email domain to a third party email systems until and unless such forwarding is required for legitimate business purposes.
- xi. Disclose information or messages from the corporate mail system only to authorized recipients for business purposes
- xii. Refrain from entering personal details or conversation into the corporate mail system as Users do not have a privacy right in any matter created on, received through or sent from the corporate email system
- xiii. Follow email etiquettes and maintain official decorum in business communication

b. Policy

- i. Certain legal risks while using the corporate email system are highlighted below:
 - An email message may go to persons other than the intended recipient. If it contains confidential or commercially sensitive information then this could be damaging to the Organization and be considered leakage of confidential information
 - Forwarding letters, files and other documents attached to emails of which the person is not an intended recipient, without permission from the sender, may be considered copyright infringement.

- User and/or the Organization shall be open to legal risk if the User sends emails with any libelous, defamatory, offensive, racist or obscene remarks
 - An email message may legally bind the Organization contractually in certain instances
 - User and/or the Organization shall be open to legal risk if a User sends an attachment that contains a virus. By opening emails and attachments from an unknown sender, a user may introduce a virus into the information systems of the organization
- ii. Email should always be regarded as potentially public information, which carry a heightened risk of legal liability for the sender, the recipient and the organizations for which they work
 - iii. Users should notify Human Resources Department or the IT Department upon learning of violations of this policy
 - iv. All Users are responsible for ensuring that the corporate mail system is used properly and in accordance with this policy. Any questions about this policy should be directed to the Human Resources Department
 - v. Even if Users have been provided password for the corporate email system, it is impossible to assure the confidentiality of any message created on, received through or sent from the corporate email system. However the Organization will implement adequate security systems of the corporate email system to safeguard its mailing platform
 - vi. The Company expressly reserves the right to monitor, access, retrieve, read any communication that is created on, received through or sent in the corporate email system to assure compliance with the IT Policies or any other policy of the Organization

c. **Operational Policy for IT team**

The IT Department shall carry out the following:

- i. Email System Security
 - Secure mail gateway shall be configured to facilitate exchange of mails to and from external mail systems over internet
 - Firewall shall be configured to ensure that only required ports are opened to/from internet
 - Gateway security solutions shall be installed for email security such that all incoming and outgoing mails are scanned for viruses
 - The Organization reserves the right to block any emails in the corporate email system
 - Adequate solutions shall be implemented to protect the Users from SPAM mail. Anti-SPAM software shall have the capability to reject emails sent from known open relay servers
- ii. ID creation, deletion & usage : The IT Department shall carry out the following:
 - Creation of mail ID for Users shall be done on receiving a formal request from HRD for email ID creation. The details provided by HRD shall be used in configuring User's email address and identification details: -
 - User shall be included in the respective mailing lists/groups as advised by the HRD
 - Group/generic email IDs should be created only after an authorization from HRD and respective Head of Departments (HoDs)
 - Access to Group IDs should be restricted to Users as approved by the group owner
 - Temporary email IDs can be created as per business requirement after approval of HoD and HRD

- The ID of the User would continue to be active and functional unless deleted on resignation, termination from employment or discretion of the Organization
 - Upon deletion of an email ID, the mailbox should be handed over to either HRD or the respective HoD
 - A group email ID shall be configured to receive all emails of a User who has left the organization for a period of 30 days to ensure business continuity. The members of the group ID shall be intimated the same by the HRD. The member can be, either:
 - A new staff who has been recruited to carry out the same role
 - An existing staff from the same department
 - Passwords for email IDs should be configured and managed in accordance to the Password Management Policy
- iii. Configuration of email IDs on multiple workstations should not be done unless approved by respective HoD
- iv. Access to email IDs other than self or sharing of email IDs is not allowed unless approved by respective HoD and HRD
- v. Email account should be created based on appropriate naming standard.
- vi. Different naming standard should be used for Users and generic ids:
- For Users: <First Name>DOT<Last Name>@ilfsindia.com
 - For Group/Generic email IDs the email IDs are created on a case by case basis.
 - In case an existing email IDs is present with the same first and last name then HRD approval is required to create an email ID in an alternate name
- vii. Internet mail (incoming): The mail ID created for Users would be automatically assigned an internet email ID and would be enabled for sending and receiving internet mail on the corporate email system
- viii. Access to corporate email system:

- Access to the corporate email system can be provided to Users for the following services:
 - Web mail
 - Mobile Phone Access - Access to be granted on a single device only
 - Blackberry Access
 - Same Time Chat

- Access to the above services will be provided to Users on a need to have basis and with prior approval of the HRD and respective HoDs

- Users who have been provided with email access on their Mobile Phones must ensure that the Organization's data stored thereon cannot be accessed by an unauthorized person in the event the device is left unattended or has been misplaced / stolen

- To prevent unauthorized access to Organization's data residing on Mobile Phones, the Users should adhere to the following guidelines:
 - Enable a startup / device lock password
 - Set a complex password that has some special characters
 - Inform the IT Department at the earliest to carry out a device wipe action on the phone as a safety measure against misuse of data on the device
 - Not share the password with anyone and must be changed at regular intervals to keep the device password secure

- Users should also take periodic backups of the phone to safeguard the data stored on the device. In the event the phone is wiped when reported, User can use the backup to restore the data stored on the device

ix. Mail Journaling:

- Mail Journaling should be done on the corporate mailing server to ensure easy retrieval in case of any user requirement
- The mail journals should be backed up regularly as per the backup policy

- The latest mail journal will be retained on the server containing the mails for the last 15 days, after which they would be archived
- x. Cross Domain certification policy:
- The mailing system of the Organization is connected to the corporate email system of its group companies to facilitate intra-company mail messaging
 - The exchange of mail across these systems is controlled by cross domain certification
 - Cross domains certification will be configured/deleted based on approval from Head – IT Infrastructure
- xi. Maintenance:
- Address book of the corporate email system including generic/group IDs will be reviewed and updated on a monthly basis to ensure only valid Users and groups are listed in the address book
 - Review of individual and generic email ID will be done with the HR while that of Group IDs will be done with the group owners
 - IDs of Users who have ceased to work with the Organization will be deleted from the address book
- xii. Disclaimer for external mails: All external mails would carry a standard system generated disclaimer as a footer of each message
- xiii. Email Signature:
- It is recommended to the Users to include email signature in all mail communications
 - The email signature could include the following:
 - Name
 - Designation
 - Organization Name
 - Contact Details

xiv. Mailbox quota:

- Every User on the corporate email system will be provided a disk quota of 300 MB. Users exceeding the disk quota will be sent a reminder mail informing them that they have exceeded the mailbox quota
- Email attachments size shall be restricted to 20 MB as per best practices and industry standards
- For attachment size larger than 20 MB, Users should use Secure File Transfer Facility provided by the Organization

xv. Access to User mailbox

- Access to another User's mailbox must be approved by HoD and HRD
- Access to existing User mailbox must be approved by HoD / CEO of the Company and by Group HR Head
- Access to the mailbox of top / senior management personnel will be given to their secretaries, based on prior approval of the concerned User
- Other than the above, access to User's mailbox by other Users is strictly prohibited and such access will not be provided by IT Department
- However, in special cases, where Head of Department requires the backup of the mailbox of his or her team members, the same would be provided, subject to approval received from the respective company's MD / CEO and Group HR Head

xvi. Definitions

- (c) IT Domain Specific Administrator: IT administrators like Network Administrator, System Administrator, Database Administrator, etc.
- (d) IT Domain Specific Manager: Team leads of the respective domains like Network Administration, IT Security Administration, System Administration, Backup Administration, etc.
- (e) SPAM: Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
- (f) Attachment: Files which are attached to an email

- (g) Disclaimer: Note stating organizations point of view towards communication over mail
- (h) Generic ID: IDs which are not attached to the name of an individual but are related to a project or a group
- (i) Journaling: Process of storing email for long term review and restoration

D. ANTI – VIRUS POLICY

1. Introduction

Malicious software or codes such as viruses, worms, trojan horses, spy ware, root-kits or any similar software programs (“**Malware**”) represents a significant threat to the performance and impacts the security levels of the Organization’s IT Systems. Thus, it is important for the Organization to safeguard the same from such attacks

2. Objective

This policy is designed to protect the Organization’s IT Systems against intrusion by Malware

3. Responsibilities

- (a) Users shall be responsible to ensure that there is no interference with the antivirus configuration and actions performed by the antivirus agent on their PCs. Users shall immediately report any suspected incident regarding any Malware to the IT Department
- (b) IT Security Administrators shall be responsible for
 - i. installation and configuration of antivirus software / solution on each User’s PC,
 - ii. handling incidents arising out of Malwares; and
 - iii. maintaining the antivirus software / solution on an ongoing basis

4. Policy Statements

(a) Antivirus Software

- i. Antivirus software shall provide continuous protection against Malware on PCs of the Organization
- ii. Features of the antivirus software shall be reviewed by the IT Department on an annual basis
- iii. Adequate licenses shall be purchased by the IT Department to ensure protection of all IT Systems

(b) Installation & Configuration

The IT Department shall:

- i. Install anti-virus software in all PCs and IT Systems
- ii. Configure anti-virus software to minimize the outbreak of any Malwares.
- iii. Configure anti-virus software to scan all internet and email traffic.
- iv. Configure anti-virus software to do a real time scan of all the files on the PCs when such files are accessed, copied or moved to ensure that all security risks are detected before they get activated
- v. Ensure that anti-virus software is password protected to prevent Users from uninstalling the software
- vi. Configure anti-virus software to scan the PCs at least once in a week which can be either when the PC boots up or during non-peak usage hours which is controlled by the IT Department
- vii. Manage all anti-virus services, real-time scan, scheduled scans, scheduled/automatic updates in User's PC
- viii. Ensure antivirus signature updates be applied to the endpoints at least on a daily basis
- ix. Ensure that infected files are quarantined if they cannot be cleaned and then deleted (after notifying the same to the User)

- x. Ensure that all files are scanned for Malware before moving or copying them
- xi. Upgrade the anti-virus software from time to time

The Users shall not:

- i. Uninstall or change the configuration of the anti-virus software
- ii. Interrupt the working of the anti-virus software or while the software is scanning documents or files on the PCs

(c) E-Mail Antivirus Policy

IT Department shall ensure that:

- i. Adequate anti-virus software to scan incoming e-mails, including attachments which scanning be implemented at gateway and on server
- ii. An email, if cannot be cleaned is deleted, if Malware is found, after giving notice to the User
- iii. Where the file pattern is related to a suspected virus, the email shall be delivered with suspected spam appended to its subject line
- iv. If the attachment or mail cannot be scanned for any reason, the e-mail must be delivered by appending the subject line with information that the e-mail was not scanned

(d) Reporting

- i. Reports from all PCs shall be reviewed on a weekly basis by the IT Department which shall cover status of anti-virus agents, anti-virus updates and Malware detected/ cleaned/quarantined. The IT Department will continue to implement system configurations to mitigate such risks
- ii. Any incidents related to non-functioning of the anti-virus software or a Malware outbreak shall be reported by any User to the IT Department taking remedial actions

5. Definitions

- (a) **Antivirus Software:** A program that monitors a computer or network to identify all major types of Malware and prevent or contain Malware incidents
- (b) **Virus:** A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk

E **PASSWORD MANAGEMENT POLICY**

1. Introduction

A password is a convenient and easy method of authentication for Users accessing the IT Systems of the Organization. This method of authentication is easily implemented, but may be subject to a number of security threats if not properly administered. A poorly chosen password may compromise the Organization's IT Systems

2. Objective

The objective of the policy is to establish guidelines for password management and usage practices for secure use

3. Responsibilities

- (a) All Users shall follow the guidelines provided below while understanding the ramifications of activities involving his/her Authentication Credentials
- (b) The IT Department shall maintain the integrity of passwords used for administrative resources and follow its guidelines as stated herein below

4. Policy Statements

All Users shall:

- (a) Use only the unique authentication credentials issued by the IT Department which consists of at least a login-ID and password for validation of the User's identity when accessing or logging into the IT Systems
- (b) Keep the login id and password confidential and not disclosure or it to any other person including such User's supervisors, personal assistants, human resources department and/or IT Department
- (c) Seek approval from the human resources department and the Head of their department for sharing the password for a specific requirement
- (d) Ensure that the passwords do not contain personal information about the User (including but not limited to name or part thereof, birth date, social security number or part thereof, license number, or staff number)
- (e) Not use passwords in any Automated Logon Process (like 'Save password' option on internet browsers) since this could be misused if PC is accessed by an unauthorized person
- (f) Not store passwords on folders in the PC
- (g) Be accountable for all activities performed using their Authentication Credentials unless the PC is hacked
- (h) Poor password complexity allows an intruder or hacker to predict or guess passwords and gain unauthorized access to the Organization's IT Systems hence password complexity is needed to make the passwords difficult to guess or retrieve
- (i) Minimum length of passwords for Users shall be 6 characters
- (j) The password shall not contain the User's account name or full name that exceed two consecutive characters
- (k) The password shall contain uppercase case characters, lower case characters, numeric digits, special characters, like @, #, &, etc.

- (l) Contact the IT Department in case of any observation of suspicious activity regarding their Authentication Credentials
- (m) Change their password
 - when prompted by the IT Systems; or
 - immediately after their password or the IT Systems that they access using their password has been, or is suspected of being compromised

The IT Department shall:

- (a) ensure that all IT Assets including workstations, PCs, software applications, operating systems, network devices and databases are protected using passwords
- (b) issue unique authentication credentials to all Users. In the first login to IT Systems, the User shall be provided with temporary password which shall have to be mandatorily changed. Authentication credentials for other applications will be communicated to Users through secure and accepted communication channels like corporate email
- (c) Issue generic credentials, as and when required for specific requirements, after seeking approval from HoD and Head – IT Infrastructure
- (d) Ensure that no passwords of Users shall be changed or shared (without the authorization of such User) with any third person
- (e) Ensure that the IT Systems mask, suppress, or obscure the display of passwords to prevent unauthorized persons from observing the same
- (f) Ensure that authentication systems store passwords in an encrypted format
- (g) Ensure accountability and security vendor default authentication credentials be changed, disabled or removed
- (h) Ensure that the password guidelines as stated herein are followed. In addition to above, the Root / Super User / Administrators shall ensure that passwords are a minimum of 8 characters
- (i) Ensure that each User's password history is maintained for 3 previous passwords

- (j) Ensure that the IT Systems automatically directs the Users to change their password at least every 90 days. If the same cannot be automated or configured for specific business requirements, shall ensure that Users manually change their passwords at least every 90 days
- (k) Reset or unlock User's account or password only on a specific request by such User and no other third person. IT Department shall exercise reasonable caution to identify Users before resetting or unlocking the account or password to avoid misuse

5. Super User / Administrator Passwords

- (a) The IT Department shall ensure that the administrative and system passwords be known or accessible to certain IT Administrators in the IT Department on a 'need to know' basis
- (b) The IT Administrators who know of the administrative or system password shall ensure that such passwords are stored securely and not shared with any unauthorized person
- (c) The IT Administrators shall immediately change the password of their administrative or System account after the password or the administrative resource has been, or is suspected of being, compromised
- (d) After any IT Administrators leaves the Organization, the Administrative or System passwords which such Administrator who was of the know, shall be immediately changed
- (e) In case of an administrative or system account where password change is not possible, additional security measures must be implemented to log and identify access attempts.

6. Definitions

- (a) **Administrative Resource:** Such as routers, switches, WAN links, firewalls, servers, Internet connections, administrative-level network operating System Accounts, Active Directory and Directory Enterprise Administrative level accounts and any other IT resource.
- (b) **Authentication:** A security procedure designed to verify that the authorization credentials entered by a User to gain access to a network or IT Systems are valid.

- (c) **Automated Logon Process:** Storing Authentication Credentials in a registry entry, macro, or function to automatically authenticate a User to a System without User intervention.
- (d) **Information System:** An information processing equipment that is recognized as "valuable" to the Organization
- (e) **System:** Software, hardware and interface components that work together to perform a set of business functions.
- (f) **System Account:** A specialized user account which have elevated privileges on the specific System running the application for which they are used.

III COMPETITION :

IL&FS believes in vigorous yet fair competition in accordance with the following principles :

1. IL&FS will not participate in any price cartel in any of its businesses that have potential to negatively affect free and fair competition
2. IL&FS will not participate in any monopolistic trade practices

IV Environmental Commitment :

All staff, in their business activities, should endeavour to adhere to the environmental aspects to the extent feasible as mentioned in Section 2.19 of the Environmental and Social Policy Framework (ESPF) Volume I, which is available on the IL&FS website

V Commitment to Stakeholders :

IL&FS recognizes the staff as one of its many stakeholders. The company shall strive to safeguard the interests of all its staff. The Company is committed to transparent disclosure of and access to information that impacts the staff

VI **Ethical conduct:**

IL&FS shall encourage and support its external stakeholders such as clients, suppliers, contractors and business partners to adopt responsible business policies and promote ethical conduct

VII **Voluntary Employment**

IL&FS does not use any forced labour, child labour, bonded labour or any other forms of involuntary labour

VIII **Work Environment**

The Company strives to provide a safe, healthy, clean and ergonomic working environment for its staff. The safety and security of the staff in the workplace is a primary concern of the Company. IL&FS respects and supports the dignity, well-being and human rights of all the staff

IX **Work-Life Balance**

1. IL&FS encourages all staff to maintain a work life balance by providing facilities such as late coming twice a month, work from home facility with the consent of the supervisor
2. IL&FS provides a fully equipped gym at BKC, Mumbai for the staff at special subsidized rates. The gym offers an assorted selection of equipment that meets the needs of the staff to keep them fit and healthy. It also offers yoga and zumba dance classes
3. At BKC, Mumbai, a bus facility is available from the nearest railway station to the office (to and fro) for all staff. An additional drop at 6:45 pm is also available for staff who work late and miss the 5:45 pm drop to the station. Similar bus facility is also available for the staff based at Gurgaon office

X Public Policy Advocacy

1. Definitions

The definitions of some of the key terms used in this Policy are given below

- (a) **Public Policy:** Public policy consists of principles that guide actions of the government, consistent with law and institutional customs
- (b) **Industry Representation:** Participation in discussion or debate on public policy on behalf of an industry sector through industry association or consultation committees formed by the government
- (c) **Staff:** includes permanent employees, people on contract, interns, trainees, and all individuals working directly for IL&FS, unless otherwise specifically mentioned
- (d) **IL&FS Representative:** means any member of the Staff or Agency retained by the Company and nominated by the Competent Authority (Any member of the Group Management Board) to represent the Company on consultative group, working group, advisory committee formed for consultations on public policy

2. Scope

- a) The objective of this policy is to set standards of conduct and establish guidelines for actions of representatives of IL&FS in public policy advocacy while ensuring compliance with all the applicable laws, particularly ensuring that the business is conducted with integrity and transparency
- b) This policy applies to all the staff of IL&FS representing the company while advocating for changes in public policy through government and industry committees.
- c) The Company believes in the conduct of the affairs of its business /in a fair and transparent manner by adopting highest standards of professionalism, honesty, integrity and ethical behaviour

- d) The Company recognizes its responsibility in contributing to the debate/discussions on public policies that will affect the stakeholders, which includes industries, community, government, but is not limited to these stakeholders

3 Policy Statement

- (a) This Policy is the Company's commitment to participation in advocacy only in a responsible manner
- (b) IL&FS Representative shall obtain prior permission from the Competent Authority before agreeing to participate in any consultation on public policy. Details such as host extending invitation, subject matter of public policy intervention, duration of engagement, significance of the public policy and proposed deliberations thereon should be communicated to the Joint MD & CEO, IL&FS through proper channel
- (c) IL&FS Representative shall proactively understand the stand of IL&FS on all issues supposed to be discussed in the consultation forum
- (d) IL&FS Representative shall prepare minutes of the public policy consultation meetings after every meeting and communicate the same to her/ his immediate supervisor/ CEO or a member of the management board as per significance of the issue

Amendments

The Company may amend or modify this Policy in whole or in part, at any time necessitated due to business needs, in a transparent manner

XI Corporate Volunteering

1. Background

- a. Volunteering demonstrates our commitment to our communities, our people and is integral to our role as a responsible business. We view contributing to society as an extension of our business aspirations. We believe volunteering contributes to civic society through active participation in building strong, inclusive and resilient communities. It underlies innovation and social change, brings together and supports the local strengths and assets of communities. This policy is designed to help support all the staff to volunteer and provide a framework of good practice
- b. For individuals, volunteering provides an opportunity to be involved in activities reflecting their interests and utilise their skills. These meaningful activities in turn promote a sense of belonging and general wellbeing. Volunteering can also be a way to explore new skills, spot potential career pathways or a way to contribute existing skills for the common good. Volunteering involvement is a two-way relationship, providing an opportunity for organisations to achieve their goals by involving the staff in their volunteering activities and for volunteers to make meaningful use of their time and skills, thus contributing to social and community outcomes

2. Definition

Volunteering is time willingly given by the staff of IL&FS and all its Group Companies and SPVs for the common good and without financial gain

3. Scope

- a. All Staff can volunteer for up to 4 days or 32 working hours annually with at least 2 consecutive days of commitment. It is recommended that preference be given to the projects that Social Inclusion Group (SIG) is working on, and thereafter to projects by our registered partner organisations. The list of all our registered partners is available with the SIG team. It will enable us to monitor and record details of contributions made

- b. All volunteering must be with the consent of your line manager. Please ensure you obtain approval in advance of any volunteering taking place. The process to securing approval is mentioned in ANNEXURE 1

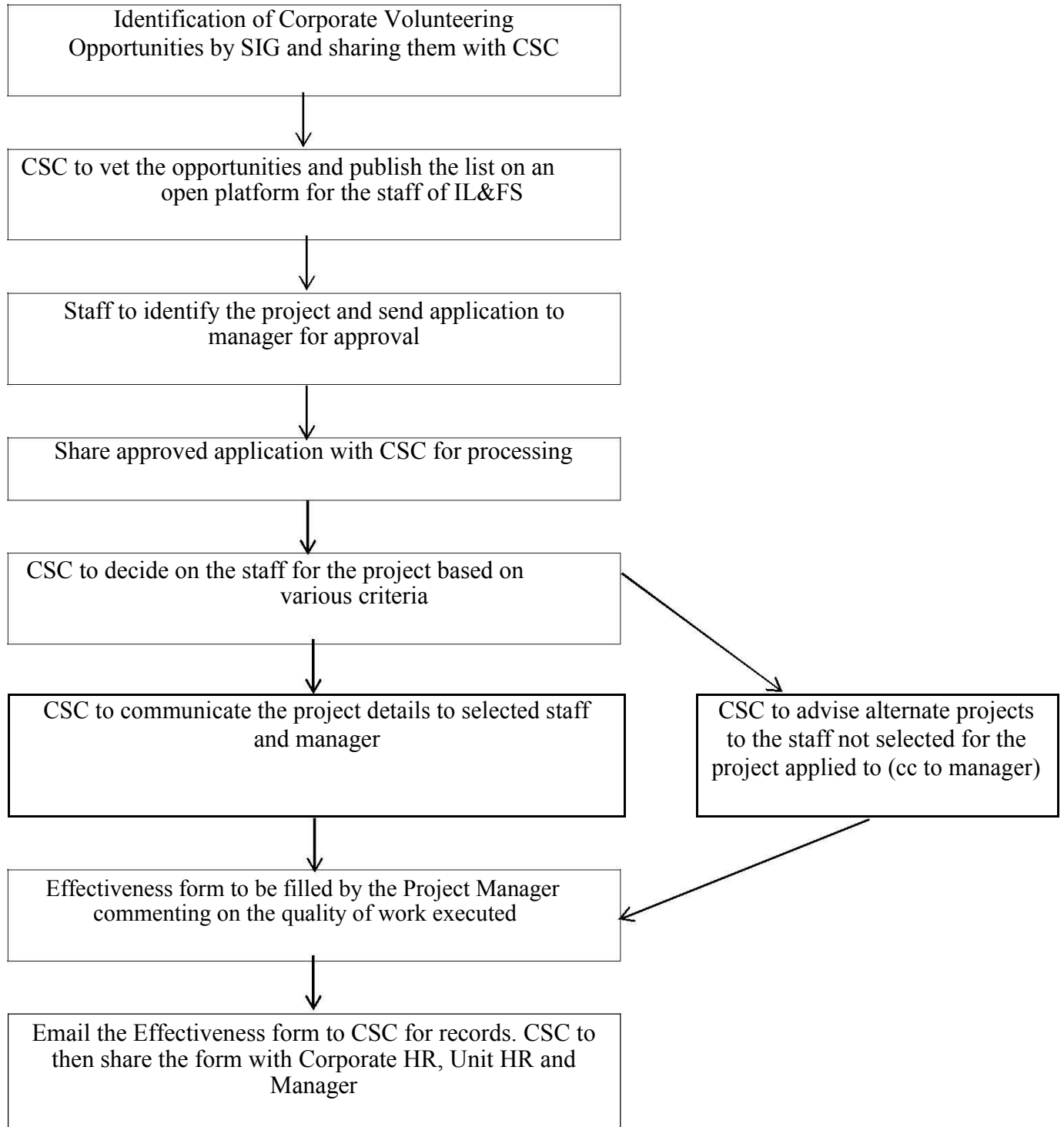
4. Developing People

- a. All volunteering can help demonstrate competencies that contribute to self-development and organisation growth. We anticipate that the volunteering projects will enable the staff to demonstrate competencies listed in our Competency Framework stated in ANNEXURE 2. We see that the staff will have ample opportunities to demonstrate some overarching competencies like Planning and Organising Skills; Effective Team Playing; Effective Communication and Effective Decision Making
- b. It will also serve as a platform for the staff to work on some specific skills that they intend to iron out while working on these projects.

5. Logistics

- a. All logistics arrangements for transport and stay will be governed by the respective company's prevailing EHB. It is imperative for the staff to seek all necessary approvals while incurring expenses for travel and food.
- b. It is recommended that the staff first opt to volunteer with Social Inclusion Group (SIG) on CSR projects with IL&FS Group companies. If a suitable project is not available with the SIG team then the concerned staff will be requested to volunteer with one of the partner organisations of SIG. Such volunteering should be undertaken in consultation with SIG.
- c. The location of volunteering should be within a reasonable distance from place of work to ensure optimal utilization of time available.

APPROVAL PROCESS



Annexure 2

IL&FS Competencies Framework

Competency		CEO & CE	% Wtg.	COO & SVP	% Wtg.	VP & AVP	% Wtg.	SM & Mgr.	% Wtg.
1	Planning and Organising Skills	-	-	5	10%	4	10%	3	15%
2	Results/Achievement Orientation	5	10%	4	10%	3	15%	2	15%
3	Effective Team Playing	-	-	-	-	4	10%	3	15%
4	Effective Communication	-	-	-	-	5	10%	4	15%
5	Organisation Commitment	-	-	5	10%	4	10%	3	10%
6	Strategic Orientation	5	10%	4	10%	-	-	-	-
7	Business / Commercial Acumen	-	-	-	-	5	15%	4	10%
8	Ability to Influence and Inspire	5	10%	4	10%	3	15%	2	10%
9	Effective Decision Making	5	10%	4	10%	3	15%	2	10%
10	Champions Change	5	10%	4	10%	-	-	-	-
11	Intra Group Coordination	5	50%	4	30%	-	-	-	-