ACCEPTABLE IT USE POLICY

for Employees of Colombo Fort Land and Building PLC and its Subsidiaries.

ABSTRACT

COMPANY IT RESOUTCES SHOULD NOT BE MISUSED

CONTENTS

1. PURPOSE AND SCOPE

The purpose of the policy governing the acceptable use of Information and IT Systems (hereinafter referred to as the “Policy”) is to outline the acceptable use of information and computer equipment/systems at all sectors within Colombo Fort Land and Building PLC and its subsidiaries (Hereinafter referred to as “CFLB”. This Policy is in place to protect the User and CFLB. Inappropriate use exposes CFLB to risks including legal issues, virus attacks, compromise of network systems and services etc.

This defines a minimum set of Acceptable Use Policies that needs to be followed by CFLB and applies to employees, contractors, consultants, temporaries, and other personnel providing services at CFLB, including all personnel affiliated with third parties (hereinafter referred to as “Users”). All Computer Hardware, Software, Operating Systems, Storage Media, Network Accounts whether owned or leased by CFLB are captured under this Policy (hereinafter referred to as “Systems”).

2. IT USAGE POLICY

CFLB provides the above-defined Systems for the effective and efficient discharge of official duties.

The following activities are prohibited with regard to the use of the systems. Under no circumstances is an employee of CFLB authorized to engage in any activity that is illegal under Sri Lankan or any International Law while utilizing the systems.

The list below is by no means exhaustive but attempts to provide a framework for activities, which shall fall into the category of unacceptable use.

2.1 UNACCEPTABLE USE

- Unauthorized use, distribution or copying of copyrighted content and material (including pictures, text, music etc.) and the installation of any copyrighted software for which CFLB does not have an active license to access corporate business systems and communicate with outside parties.

- Sharing of user accounts (company username/password pairs) and the respective user will be responsible for any activity carried out using an account assigned to him/her. Any exceptions required as a result of business requirements is to be documented and required permission sort from Sector MD.

- Sharing Files/Folders without proper access restrictions.

- Leaving the computer in unlock mode when physically not present.

- Storing non-business related data on the centrally mapped network drives.

- Installing unauthorized hardware and accessories.

- Installing or playing games on Systems.

- Creating, Distributing or Viewing Pornographic or obscene material

- Use of Systems for the furtherance of any political, religious agenda

- Effecting security breaches or disruptions of network communication: Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless these duties are within the scope of the User’s regular duties (IT Administrators). For purposes of this section, "disruption" includes, but is not limited to, network sniffing, network monitoring, ping floods, packet spoofing, denial of service, and forged routing information, Introduction of malicious programs such as viruses, Trojans, worm and Spyware etc.

- Any action using Systems that are aimed at disrupting or harassing another employee or other outside party.

- Operating a computer without a virus scanner which is updated automatically on regular basis.

3. PASSWORD POLICY

Passwords are an important aspect of security of the Systems. They are the front line of protection for User Accounts. A poorly chosen password may result in the compromise of CFLB's entire network. Therefore it is necessary to establish a policy for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3.1. GENERAL

- All system-level passwords (e.g., root, enable, DBA/Network admin, application administration accounts, etc.) must be changed every 60 days.

- All user-level passwords must be changed at least every 60 days.

- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.

- Passwords must not be inserted into email messages or other forms of electronic communication.

- All user-level and system-level passwords should contain at least eight characters, including one upper case letter, one special character and one numeric.

3.2 PASSWORD PROTECTION STANDARDS

- Do not use the same password for CFLB account as for other non- CFLB access. (e.g., Personal ISP account, Internet Banking, Benefits, etc.). Where possible, do not use the same password for various CFLB access needs.

- Do not share CFLB passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential CFLB information.

- It is strictly prohibited to share user accounts for any system. If an employee with high level privileges will be away from work for any reason, there must be another employee who will be delegated these privileges and responsibilities to carry out the work. This should be done through a separate user account.

  Here is a list of "don'ts":

  - Refrain from using your username as your password.
  - Refrain from revealing your password to anyone including your Superiors, IT administrators or family members.
  - Do not reveal a password in an email message or over the phone.
  - Refrain from talking about a password in front of others.
  - Refrain hinting at the format of a password (e.g., "my family name").
  - Refrain from revealing a password or details about it on questionnaires or security forms.
  - If someone demands a password, refer him or her to this document or have him or her call someone responsible in your sector IT.
  - Do not use the "Remember Password" feature of applications (e.g. Email, Internet Proxy).
  - Again, do not write passwords down and store them anywhere. Do not store passwords in a file on ANY computer system (including PDA‟s, Mobile Phones or similar devices).
  - Refrain from using at least the three previously used passwords when the password is being changed.

- If an account or password is suspected to have been compromised, report the incident to the responsible person within your sector IT and change all passwords.

4. E-MAIL USAGE POLICY

The purpose of this policy is to ensure the proper use of CFLB email system and make users aware of what the company deems acceptable and unacceptable use of its email system. The Email facility is a business communication tool and users are required to use this tool in a responsible, effective and lawful manner.

4.1. LEGAL ISSUES

It is important that users are aware of the legal risks of an e-mail:

- If you originate emails with any libelous, defamatory, racist or obscene remarks and or content, you and CFLB can be held liable.
- If you forward emails (originated by another) with any libelous, defamatory, racist or obscene remarks, you and CFLB can be held liable.
- If you unlawfully (i.e. without the consent of the party disclosing the information to you) forward confidential information, you and CFLB can be held liable.
- If you unlawfully forward or copy messages without permission, you and CFLB can be held liable for copyright infringement even though the copyright so infringed is not of the party who sent you the email.
- If you send an attachment that contains a virus, worms, Trojans or hoaxes you and CFLB can be held liable.

The disclaimer should carry the following meaning and be automatically added to any E-mail sent to external parties.

Disclaimer

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the original sender. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

4.2. UNACCEPTABLE USE

- It is strictly prohibited to originate or forward emails containing libelous, defamatory, racist, religious, or obscene remarks.
- Do not forward a message without acquiring permission from the sender first. (User discretion is advised until a formal information classification policy is in place).
- Do not send unsolicited email messages.
- Do not distribute pornographic or obscene material through e-mail either internally or externally.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person’s email account.
- Do not copy a message or attachment belonging to another user without permission of the originator.
- Do not disguise or attempt to disguise your identity when sending mail.
- Do not use e-mail for communications of a sensitive nature.
- Do not send emails with large attachments. The maximum size of an email that could be sent through corporate systems is limited to 8MB. Any exceptions to email size should be authorized by Sector Heads based on exceptional business requirements.
- Do not send emails with Music /sound, Executable and Multimedia as attachments.
- Do not send emails with attachments to number of users before consulting a responsible person in you sector IT.
- Number of external recipients should not exceed 50 per Email.

All messages distributed via the Company’s email system, even personal emails, are CFLB property.

4.3. USAGE MONITORING

Your email usage may be monitored without prior notification and monthly reports will be submitted if required. This includes:

- Number of emails sent and received.
- Number of bytes transferred and received.

Above message statistics provides summary information on the distribution of message sizes created and received by individual users. These statistics will be used in assessing the appropriateness of end user email habits providing opportunities to educate users on sending smaller links for compressing files in advance of email.

Sent Distribution

The Sent Distribution report provides a breakdown of the distribution of message sizes sent across the corporate mail server and summarizes this information at the corporate level. This report answers the question, ''On average, what size messages do users send?''.

Received Distribution

The Received Distribution report provides a breakdown of the distribution of message sizes received across the corporate mail server and summarizes this information at the corporate level. This report answers the question ''On average, what size messages do users receive?''.

5. INTERNET USAGE POLICY

Internet access is granted to Users to facilitate the efficient discharge of their duties as with other IT resources. This should be used extensively by the employees for official purposes and should not be abused.

The Internet can be a magnificent source of detailed, current information that can enhance employee productivity. This policy hopes to guide Users to make use of this resource in a way that will help them achieve their official goals.

Users are advised not to use the Internet for any purpose which would reflect negatively on CFLB. Internet Access may be requested through the Head of the department.

5.1. UNACCEPTABLE USE

- Internet access is granted only through the corporate network (and proxy) and attempting to gain Internet access through unauthorized means (installing unauthorized modems etc.) is strictly prohibited.
- User shall not:
- Browse, distribute or download pornographic or obscene material in any form.
- Engage in criminal activity including but not limited to hacking, cracking, sniffing or disrupting CFLB or third party systems.
- Access unauthorized web based third party e-mail accounts such as Yahoo, Hotmail, Gmail, SLTNet etc.
- Use IM clients other than approved and authorized by Individual Sector MD.
- Visit or engage in online gambling activities or other gaming activities
- Access to any Social Media networks unless approved and authorized by Individual Sector MD.
- Engage in activity that will infringe the copyrights of others by sharing/distributing/downloading of copyrighted material such as but not limited to music through Peer-to-Peer applications. In addition these applications will use up a lot of bandwidth and this will hinder use of the network by others.
- Install server applications accessible from the Internet is strictly forbidden to general users. If such use is required, prior approval needs to be sought.
- Share information with third party.

6. MONITORING

- CFLB employees shall have no privacy in anything they store, send or receive on the Company's Systems and information could be accessed by an authorized person with prior approval.
- CFLB may monitor any activity without prior notice.
- CFLB is not obliged to monitor activity.

7. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action.

This policy may be modified as and when required and the users will be informed appropriately.