IT POLICY

IT Policy for Colombo Fort Land and Building PLC and its subsidiary companies

24.08.2015

RESPONSIBILITY OF ADHERENCE

This document specifies the CFLB Group IT policy which must be adhered to by ALL business units, as a minimum set of guidelines. The compliance will be the responsibility of the individual Sector Head.

CONTENTS

1. GROUP CONNECTIVITY

There should be an industry standard data communication /connectivity infrastructure for the whole group and the connectivity should be controlled by appropriate access control mechanisms.

The core data communication infrastructure (This excludes Sector Local Area Networks and any proprietary infrastructure (if applicable)) of the group should be managed by one single party (Central Services) and they should be accountable for proper and secure implementation of the same with detailed documentations.

The group corporate network should connect to the Internet ideally from only one point where all the necessary security (FW with AI/IPS/Bandwidth Management/ Virus-walls etc.) and controls be implemented and there should be dedicated qualified staff managing the setup. If there are more than one point connected to the Internet that has to be for a very specific reason only and with the approval of sector MD.

All means of Remote access to the Corporate network and resources will only be permitted provided that authorized users are authenticated, data is encrypted across the network, and privileges are restricted. Ideally there should be only one remote access point to the corporate network. If any other remote access point to the corporate network is required, it has to be for a very specific reason only and with the approval of sector MD.

2. ACCESS REQUIREMENTS / RESOURCE UTILIZATION

Access to the resources on the network must be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.

Access control requirements for networks should be assessed, defined and documented by the requestor and the provider.

Users and service providers should be given a clear statement of the business requirements to be met by access controls.

Access control requirements for applications, should be requested by the requestor. This should then be assessed, defined and documented by the approver and handed to provider to grant access and document.

Procedures for monitoring the use of information processing facilities are to be established. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized.

Centralized storage and computing resources should be used wherever possible to effectively and efficiently manage computing resources and for implementing better administrative controls, Disaster recovery mechanisms. This will help to eliminate wasted storage / computing resources scattered throughout the corporate and consolidation of IT resources wherever possible will help to better utilize resources.

All Computer/User accounts of staff leaving employment should be informed through company's HR exit procedure to Service Providers Internal/External) in a timely manner for necessary actions.
"Administrative" privileges of user desktops, laptops should ONLY rest with the designated system administrators of the respective sectors. Any exception to this should be authorized in writing by the sector MD through a policy waiver.

Sharing of user accounts should not be allowed, unless for a very specific business reason and approved by the Sector MD.

3. INDIVIDUAL SECTOR NETWORKS / SYSTEM MANAGEMENT

All the individual networks within sectors must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions.

System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

Individual sector IT should take maximum precautions to avoid unauthorized services/activities being used and unauthorized devices being connected to their network including ALL portable computing devices.

Without exception, Anti-Virus software is to be deployed across all PCs with regular virus definition updates and scanning across servers, PCs and laptop computers.

All the individual networks within sectors should have a centrally managed Virus protection system. The centrally managed Virus protection system should update itself with the latest signatures at least once every day.

Systems within sectors are to be managed by a suitably qualified systems administrator who is responsible for overseeing the day to day running and security of the systems.

System Administrators must be fully trained and have adequate experience in the wide range of systems and platforms used by the organization. In addition, they must be knowledgeable and conversant with the range of Information Security risks which need to be managed.

System documentation is a requirement for all the organization's information systems including hardware resources. Such documentation must be kept up- to-date and be available.

4. BACKUP & RECOVERY

Backup of the data files and the ability to recover such data is a top priority. Sectors should ensure that the frequency of such backup operations and the procedures for recovery meet the needs of the business.

The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved.

Business critical information and data stored on Desktop/Laptop or portable computers must be backed up regularly. It is the responsibility of the Sector IT to ensure that this takes place on a regular basis.

Business owners should conduct a “Business Impact Analysis” of their systems at regular intervals or when there is a significant change to the business processes to ascertain the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) of their systems.

Business Owners of the information systems must ensure that disaster recovery plans for their systems are developed, tested, and implemented to meet the RTO and RPO requirements.

5. SOFTWARE DEVELOPMENT / MODIFICATION

Software developed for or by the organization must always follow a formalized development process which itself is managed under the project in question. The integrity of the operational software code must be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures.

Emergency amendments to software are to be discouraged, except in circumstances designated by the business owner as 'critical'. Any such amendments must strictly follow agreed change control procedures.

All proposed system enhancements must be business driven and supported by an agreed Business Case. Ownership (and responsibility) for any such enhancements will ultimately rest with the business owner of the system.

Formal change control procedures must be utilized for all amendments to systems. All changes to programs must be properly authorized and tested in a “test” environment before moving to the “live” environment.

All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the “live” environment unless supporting documentation is available.

Vendor developed software must meet the User Requirements Specification and offer appropriate product support.

6. IT EQUIPMENT / SOFTWARE & THIRD PARTY INVOLVEMENTS

All Desktop, Laptop and server procurements should be branded and with licensed operating systems.

Use of unlicensed software on Desktops / Laptops and servers is prohibited except for evaluation purposes and should be documented.

Services provided by third parties should be governed by approved service level agreements that are monitored and enforced.

Service level management concepts are to be applied to all deliveries of services from third parties. This will require third parties to meet all security and service controls, service definitions and agreed service levels.

Any changes that are to be made to services provided by third parties are to be agreed prior to the changes taking place and the service level agreements amended accordingly.

7. IT ASSETS AND MEDIA DISPOSAL / PROCUREMENT

Individual sector should identify and endorse the need to replace / dispose equipment which are deem not suitable to operate within the sectors for justifiable reasons such as defects that cannot be feasibly repaired, require installation of application and system software which require higher specifications, running system software which has gone out of vendor support etc.

All IT assets should be disposed by either trading-in against cost or negotiated discount rate of replacement or associated item, sold by auction or by a third party, sold to a staff member or disposed of as per socially acceptable environmental guidelines.

All IT media shall be securely disposed of by authorized users when it is no longer required by physically destroying the IT media in socially acceptable environment guidelines.

Ensure that any form of IT media that contains CONFIDENTIAL data is sanitized and disposed of in a manner that the content could not be recreated.

IT Asset procurement should comply with a central preferred supplier / procurement strategy where applicable.