Annex I

Basic Cyber Security Controls for Primary (Urban) Cooperative Banks (UCBs)

1) Inventory Management of Business IT Assets

1.1 UCBs should maintain an up-to-date business IT Asset Inventory Register containing the following fields, as a minimum:

a. Details of the IT Asset (viz., hardware/software/network devices, key personnel, services, etc.)
b. Details of systems where customer data are stored
c. Associated business applications, if any
d. Criticality of the IT asset (For example, High/Medium/Low)

1.2 Classify data/information based on sensitivity criteria of the information

1.3 Appropriately manage and provide protection within and outside UCB/network, keeping in mind how the data/information is stored, transmitted, processed, accessed and put to use within/outside the UCB's network, and level of risk they are exposed to depending on the sensitivity of the data/information

2) Preventing access of unauthorised software

2.1 Maintain an up-to-date and preferably centralised inventory of authorised software(s)/approved applications/software/libraries, etc.

2.2 Put in place a mechanism to control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. Also, put in place a mechanism to block/prevent and identify installation and running of unauthorised software/applications on such devices/systems.

2.3 The web browser settings should be set to auto update and consider disabling scripts like JavaScript, Java and ActiveX controls when they are not in use.

2.4 Internet usage, if any, should be restricted to identified standalone computer(s) in the branch of a UCB which are strictly separate from the systems identified for running day to day business.

3) Environmental Controls

3.1 Put in place appropriate controls for securing physical location of critical assets (as identified by the UCB under its inventory of IT assets), providing protection from natural and man-made threats

3.2 Put in place mechanisms for monitoring of breaches/compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc. Appropriate physical security measures shall be taken to protect the critical assets of the UCB.

4) Network Management and Security

4.1 Ensure that all the network devices are configured appropriately and periodically assessed to ensure that such configurations are securely maintained.

4.2 The default passwords of all the network devices/systems should be changed after installation.

4.3 Put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.

4.4 Critical infrastructure of UCB (viz., NEFT, RTGS, SWIFT, CBS, ATM infrastructure) should be designed with adequate network separation controls

5) Secure Configuration

5.1 The firewall configurations should be set to the highest security level and evaluation of critical device (such as firewall, network switches, security devices, etc.) configurations should be done periodically.

5.2 Systems such as Network, application, database and servers should be used dedicatedly for the purpose for which they have been set up.

6) Anti-virus and Patch Management

6.1 Put in place systems and processes to identify, track, manage and monitor the status of patches to servers, operating system and application software running at the systems used by the UCB officials (end-users).

6.2 Implement and update antivirus protection for all servers and applicable end points preferably through a centralised system.

7) User Access Control / Management

7.1 Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a 'need to know' and 'need to do' basis.

7.2 Passwords should be set as complex and lengthy and users should not use same passwords for all the applications/systems/devices.

7.3 Remote Desktop Protocol (RDP) which allows others to access the computer remotely over a network or over the internet should be always disabled and should be enabled only with the approval of the authorised officer of the UCB. Logs for such remote access shall be enabled and monitored for suspicious activities

7.4 Implement appropriate (e.g. centralised) systems and controls to allow, manage, log and monitor privileged/super user/administrative access to critical systems (servers/databases, applications, network devices etc.)

8) Secure mail and messaging systems

8.1 Implement secure mail and messaging systems, including those used by UCB's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.

8.2 Document and implement email server specific controls.

9) Removable Media

9.1 As a default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorised for defined use and duration of use.

9.2 Secure the usage of removable media on workstations/PCs/Laptops, etc. and secure erasure/ deletion of data on such media after use

9.3 Get the removable media scanned for malware/anti-virus prior to providing read/write access

10) User/Employee/Management Awareness

10.1 Communicate to users/employees, vendors & partners security policies covering secure and acceptable use of UCB's network/assets including customer information/data, educating them about cyber security risks and protection measures at their level.

10.2 Conduct awareness/training for staff on basic information security controls (Do's and Don'ts), incident reporting, etc.

10.3 Board members may be kept updated on basic tenets/principles of IT risk/cyber security risk at least once a year.

10.4 The end-users should be made aware to never open or download an email attachment from unknown sources

11) Customer Education and Awareness

11.1 Improve and maintain customer awareness and education with regard to cyber security risks

11.2 Educate the customers on keeping their card, PIN etc. secure and not to share with any third party

12) Backup and Restoration

Take periodic back up of the important data and store this data 'off line' (i.e., transferring important files to a storage device that can be detached from a computer/system after copying all the files).

13) Vendor/Outsourcing Risk Management

13.1 All the outsourcing service level agreements (SLAs) signed with the vendors must clearly mention the responsibility of the UCB and vendor in case of any failure of services

13.2 The agreements must clearly mention the grievance redressal mechanism to resolve customer complaints

13.3 Vendors' service level agreements shall be periodically reviewed for performance in security controls

----------X----------