INFORMATION SECURITY POLICY

SYSTEM AND DATA ACCESS AND CONTROL POLICY
(CHAPTER 2)

ENSURE THAT ALL INFORMATION ARE PROTECTED FROM UNAUTHORIZED ACCESS BY OBSERVING THE FOLLOWING:

SEC.1
ACCESS

- ACCESS BY AUTHORIZED UP STAFF ONLY
- STORAGE LOCATIONS KEPT SECURED AND LOCKED
- TRACK HISTORICAL ACCESS TO PAPER-BASED FILES
- PERSON-IN-CHARGE OF DATA AND STORAGE DEVICE SHALL BE RESPONSIBLE AND ACCOUNTABLE AT ALL TIMES

SEC.2
ONLINE ACCESS

- ACCESS IS THRU OFFICAL DEVICES ONLY
- MUST HAVE A STRONG PASSWORD OR PASSPHRASE
- MUST HAVE AN ACCESS CONTROL LIST
- ENCRYPTED DATA

SEC.3
REMOTE ACCESS

- DOCUMENTED ACCESS REQUEST
- DEVICES MUST BE EQUIPPED WITH APPROPRIATE SECURITY MEASURES

SEC.4
REMOTE DISCONNECTION/ WIPING

- RECOMMENDED THAT DEVICES ARE ENABLED AND READY FOR THESE FEATURES

SEC.5
GUEST ACCESS

- PROVIDE GUEST NETWORK FOR GUESTS OR THIRD PARTIES
- ACCESS IS SUBJECT TO UP'S ACCEPTABLE USE POLICY

SEC.6
VPN

- VIRTUAL PRIVATE NETWORKS SHOULD BE SET UP FOR REMOTE ACCESS TO UP DILIMAN NETWORK, SYSTEMS, OR SERVERS

INFORMATION SECURITY POLICY

PASSWORD/PASSPHRASE POLICY
(CHAPTER 6)

PASSWORD

is a string of characters, usually comprised of letters, numbers, and other symbols, that are used to authenticate the identity of a particular user or verify one's access authorization.

EXAMPLES:

Weak:
12345
Asdfghjkl

Strong:
YouN33dCapital
Refreeg1rat0r

EXAMPLES:

Weak:
HelloThere
LuckyMe

Strong:
LeBronJamesBondPaper
HairyPotterAndThePilosopoStoned

PASSPHRASE

is a sequence of words or text that, similar to a password, a user employs to authenticate his identity. For security purposes, it is generally longer than passwords but are easier to remember.

BACKUP POLICY
(CHAPTER 7)

HOW TO BACK UP

Back up data in three different platforms or storages that are not stored in a single location.

WHAT TO BACK UP

Units and offices are required to maintain a backup file for all the personal data it holds. Files that have been changed or modified must also be backed up regularly.

DATA RECOVERY CAPABILITY

It is highly advised that regular testing, assessment, and evaluation be conducted to check whether the back up systems employed by the units and offices can effectively and timely save the data as well as retrieve and restore the same.