

GENERAL INSTRUCTIONS FOR IT SECURITY AWARENESS

(TO BE DISPLAYED ON ALL NOTICE BOARDS OF EVERY DEPTS / OFFICES / SECTIONS)

- FOR PC / LAPTOP AND DATA PROTECTION:

- **USE PC / LAPTOP PROVIDED BY THE COLLEGE ONLY.**
- **DO NOT CONNECT YOUR PERSONAL PC / LAPTOP/TAB/MOBILE TO THE COLLEGE NETWORK WITHOUT PROPER PERMISSION FROM THE AUTHORITY.**
- **USE LEGAL OPERATING SYSTEM AND APPLICATIONS ON YOUR PC / LAPTOP.**
- **USE STRONG PASSWORDS AS LONG AS POSSIBLE MIN 8 CHARS, WITH MIXED-CASE LETTERS, INCLUDE DIGITS, NOT BE BASED ON ANY PERSONAL INFORMATION, NOT BE BASED ON ANY DICTIONARY WORD, IN ANY LANGUAGE.**
- **DO NOT SHARE / DISCLOSE YOUR SYSTEM PASSWORD TO OTHER STAFF.**

GENERAL INSTRUCTIONS FOR IT SECURITY AWARENESS

(TO BE DISPLAYED ON ALL NOTICE BOARDS OF EVERY DEPTS / OFFICES / SECTIONS)

- FOR PC / LAPTOP AND DATA PROTECTION:

- **DO NOT SAVE YOUR PASSWORDS ON THE HARD DISK / INTERNET BROWSER.**
- **CHANGE PASSWORDS AT REGULAR INTERVALS. NEVER USE THE SAME PASSWORD TWICE.**
- **KEEP THE SYSTEM SCREEN SAVER ENABLED WITH PASSWORD PROTECTION.**
- **INSTALL ONLY LEGAL ANTI-VIRUS SOFTWARE PROVIDED BY THE COLLEGE AND UPDATE IT REGULARLY.**
- **KEEP BACKUP COPY OF YOUR IMPORTANT DATA ON PEN DRIVE, CD, DVD ETC.**

GENERAL INSTRUCTIONS FOR IT SECURITY AWARENESS

(TO BE DISPLAYED ON ALL NOTICE BOARDS OF EVERY DEPTS / OFFICES / SECTIONS)

- FOR PC / LAPTOP AND DATA PROTECTION:

- **ALWAYS BACKUP THE DATA BEFORE LEAVING OFFICE.**
- **DO NOT KEEP ANY SENSITIVE DATA SUCH BANK PASSWORDS ON THE SYSTEM. KEEP THEM SECURE FROM EVERYONE.**
- **SYSTEM SHOULD BE PROPERLY SHUT DOWN BEFORE LEAVING THE OFFICE.**
- **LOG-OFF THE SYSTEM IF YOU ARE LEAVING YOUR SEAT.**
- **FOOD AND DRINKS SHOULD NOT BE PLACED NEAR SYSTEMS. CUP OF TEA/ COFFEE OR WATER GLASS SHOULD NOT BE ON CPU OR MONITOR OR KEYBOARD.**

GENERAL INSTRUCTIONS FOR IT SECURITY AWARENESS

(TO BE DISPLAYED ON ALL NOTICE BOARDS OF EVERY DEPTS / OFFICES / SECTIONS)

- FOR ACCESSING INTERNET:

- **ALL SYSTEMS REQUIRED INTERNET ACCESS BE SECURED THROUGH COLLEGE FIREWALL.**
- **NO OPEN INTERNET ACCESS WITHOUT AUTHENTICATION THROUGH FIREWALL ALLOWED.**
- **AUTHENTICATION WILL BE ONLY VIA A SECURE PASSWORD.**
- **PASSWORDS SHOULD BE COMPRISED OF A MIX OF UPPER AND LOWER CASE ATLEAST 8 ALPHANUMERIC CHARACTERS.**
- **PASSWORDS SHOULD BE COMPRISED OF A MIX OF UPPER AND LOWER CASE ATLEAST 8 ALPHANUMERIC CHARACTERS.**

GENERAL INSTRUCTIONS FOR IT SECURITY AWARENESS

(TO BE DISPLAYED ON ALL NOTICE BOARDS OF EVERY DEPTS / OFFICES / SECTIONS)

- FOR ACCESSING INTERNET:

- EACH USER BE ENSURE THAT THEIR PASSWORD IS NOT DISCLOSED TO ANYONE. IN THE RARE EVENT THAT A MEMBER OF THE INTERNET SUPPORT STAFF REQUESTS A USER'S PASSWORD FROM THEM TO RECTIFY A PROBLEM WITH THEIR SYSTEM, THE USER SHOULD CHANGE THEIR PASSWORD IMMEDIATELY AFTERWARDS.
- USERS SHOULD NEVER SEND THEIR INTERNET PASSWORDS OR OTHER IDENTITY INFORMATION VIA EMAIL, FAX, POST ETC.
- ONLY USE INTERNET ASSIGNED IP ON THE SYSTEMS. DO NOT USED MULTIPLE IPS ON THAT SYSTEMS.
- ALL PC / WORKSTATIONS / LAPTOPS INTERNET ACCESS MUST HAVE LEGAL ANTIVIRUS/ANTI-MALWARE SOFTWARE INSTALLED.

GENERAL INSTRUCTIONS FOR IT SECURITY AWARENESS

(TO BE DISPLAYED ON ALL NOTICE BOARDS OF EVERY DEPTS / OFFICES / SECTIONS)

- FOR ACCESSING INTERNET:

- **DO NOT ACCESS NON-ACADEMIC RELATED WEBSITES.**
- **MOST OF NON-ACADEMIC RELATED WEBSITES ARE BLOCKED BY THE FIREWALL, DO NOT REQUEST FOR OPENING THESE BLOCKED WEBSITES.**
- **DO NOT ACCESS NON-SECURED WEBSITES AS THEY HAVE BEEN HACKED OR INFECTED BY VIRUSES, MALWARES ETC.**
- **ILLEGAL NETWORK APPLICATIONS, HACKING TOOLS ETC SHOULD NOT INSTALLED ON SYSTEMS.**