SECURITY PLANNING

PRESENTED BY:
SHWETA SHARMA

1. PURPOSE

To ensure the security of **organisation** network and to establish appropriate security requirements and restrictions on accessing and using organisation computers, computer systems and networks and safeguarding organisation information.

1.1 ENSURE AVAILABILITY

Ensuring information is available when it is required. Data can be held in many different areas, some of these are:

- Network Servers
- Personal Computers and Workstations
- Laptop and Handheld PCs
- Removable Storage Media (Floppy Disks, CD-ROMS, Zip Disks, Flash Drive)
- Data Backup Media (Tapes and Optical Disks)

1.2 ENSURE THAT THE NETWORK IS FOR USERS

A formal relationship between Organisation Computer Services and a user of those services that allow the user to access and use university computer systems for legitimate academic or other university work. Accounts are established in accord with the provisions of university policies that govern access and use of these computer systems.

1.3 PRESERVE INTEGRITY AND CONFIDENTIALITY

Protecting information from unauthorized modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate and complete.

Protecting information from unauthorized disclosure like to the press, or through improper disposal techniques, or those who are not entitled to have the same.

2 THE POLICY

The **C-DAC** information network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality.

2.1 POLICIES FOR STUDENTS

Using Floppies/ CD/ Flash Drives

- Floppy should be used in consultation with system administrator/in-charge computer centre and should be scanned before use.
- Unofficial Floppies, CDs or Flash Drives should not be used in computer centre.

2.1 POLICIES FOR STUDENTS

Password

- Keep the system screen saver enabled with password protection.
- Don’t share or disclose your password.
- User should not have easily detectable passwords for Network access, screen saver etc.
- A strong password must be as long as possible, include mixed-case letters, include digits and punctuation marks, not be based on any personal information, and not be based on any dictionary word, in any language.
- Never use the same password twice.
- Change password at regular intervals.

2.1 POLICIES FOR STUDENTS

Backup

- Backup should be maintained regularly on the space provided on central server of the department or on the storage media as per department policy.
- Keep paper copy of server configuration file.
- Keep removable media in a secure location away from the computer.
- Always backup the data before leaving the workstation.
- For sensitive and important data offsite backup should be used.

2.1 POLICIES FOR STUDENTS

Physical Safety of System

- Report any loss of data or accessories to the System Administrator/in-charge computer centre.
- Keep the system and sensitive data secure from outsiders.
- Install UPS system with adequate battery backups to avoid any data loss or corruption due to power failure.
- Log-off the system if you are leaving your seat.
- Never remove the cables when your PC is powered ON since this can cause an electrical short circuit.
- Always use mouse on mouse pad.

2.1 POLICIES FOR STUDENTS

Computer Files

- Never download or run attached files from unknown email ID.
- Always keep files in the computer in organized manner for easy accessibility. If required create new folders and sub-folders.
- Avoid creating junk files and folders.
- System files and libraries should not be accessed as it can cause malfunctioning of system.

2.1 POLICIES FOR STUDENTS

General Instructions

- Follow instructions or procedures that comes from System administrator/In-charge computer centre time to time.
- Please intimate System administrator/In-charge computer centre in case of system malfunction.
- Students should always work on his/her allotted machines. In case of any urgency/emergency user may use other's machine with consultation of System administrator/In charge computer centre.
- Antivirus software should be updated timely in consultation with System Administrator/In-charge computer centre.
- Don't give others the opportunity to look over your shoulder if you are working on sensitive data/contents.
- Do not install or copy software on system without permission of System administrator/In-charge computer centre.
- Food and drinks should not be placed near systems. Cup of Tea/ Coffee or water glass should not be on CPU or Monitor or Key Board.
- Always power off the system when cleaning it.
- Never use wet cloth for wiping the screen.
- Never shut the system down while programs are running.
- Never stack books/ files or other materials on the CPU.

3. LOG MANAGEMENT AND MONITORING

Network manager shall configure IT Resources to record and monitor network security incidents, events and weaknesses. IT resource administrators shall regularly review and analyse these logs for indications of inappropriate or unusual activity.

The Network Manager is responsible for ensuring that a log of all faults on the network is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

4. DATA BACKUP AND RESTORATION

The Network Manager **is** responsible for ensuring that backup copies of network configuration data are taken regularly at user level, application level and system level.

Documented procedures for the backup process and storage of backup tapes will be produced and communicated to all relevant staff.

All backup tapes will be stored securely and a copy will be stored off-site.

Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.

Users are responsible for ensuring that they backup their own data to the network server.

5. USER RESPONSIBILITIES, AWARENESS & TRAINING

The Organisation's students, faculty, staff, permanent and temporary employees and, where appropriate, contractors and third party users shall receive security awareness training and regular updates on the University's policies, rules and procedures, as relevant for their role at the University.

6. SECURITY AUDITS

It is the responsibility of all Departments officers to place an appropriate system of internal audit, which provides an independent assessment of security policies. To execute these policies, internal audit should also be done and reports/documents based on these audits should be generated. The system administrator or officer will be responsible for internal Audit within the department and operations of their sub dept. When requested and for the purpose of performing an audit, any access needed will be provided to members of External Audit team.

7. BUSINESS CONTINUITY & DISASTER RECOVERY PLANS

The Organisation shall develop and periodically review, test and update a formal, documented, contingency plan based on a business impact analysis that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Organisation administrative units and entities, escalation procedures and compliance, as well as develop and periodically review, test and update formal, documented procedures to facilitate the implementation of the contingency plan.

Where appropriate, the Organisation must develop contingency plans that allow physical access to facilities in order to recover data and resume operations in the event of an emergency or disaster (for example, if card access to the data centre were to fail).

As needed, the Organisation shall establish (and implement as necessary) procedures to enable continuation of critical business processes for protection of the security of information while operating in emergency mode.

8. INFORMATION SECURITY OFFICER'S RESPONSIBILITIES

Planning: Security officers assess their organization's infrastructure and data to identify vulnerabilities caused by weaknesses or flaws in software and hardware that could expose the infrastructure to a security breach. They also evaluate the effectiveness of existing **security measures, such as firewalls, password policies and intrusion-detection systems**. They make **recommendations to improve security** based on their assessments and knowledge of current and emerging threats.

Policies: Balancing essential access to data and systems with high levels of security is a major challenge for officers. They develop policies that give varying levels of access to corporate applications, systems and data, and they monitor access to ensure compliance.

Training: To reinforce the importance of information security, officers **run training and awareness programs for students.** They demonstrate good practices and explain the risks of poor security practices, such as using weak passwords. They may caution against including sensitive data in emails or using data that is not encrypted in laptops or other mobile devices that could be lost or stolen.

Security Solutions: Officers select and **install security products, such as firewalls, anti-virus software** and software to protect the network. They install software to monitor security across all corporate networks, computers and storage devices, so that they can quickly identify attacks and respond to any alerts. Officers also carry out tests, such as simulated attacks, on their own security systems to ensure that there are no weaknesses.

Updating: Security officers update anti-virus software and monitor employee access levels. Officers must minimize the risk of damage from security breaches by putting a business continuity or disaster recovery plan in place. They might set up duplicate data-storage facilities in another location, for example, so that the latest data is available even if there is a major security attack.


Thank
you!!