Safe Operation Procedure (SOP)

DSP, Control, VLSI and Simulation Laboratories, Department of EEE, BUET

1. Purpose

This Standard Operating Procedure (SOP) establishes safe and responsible operating practices for students, teachers, and staff working in the **Electronic Circuits Simulation Laboratory**, **Robert Noyce Laboratory**, **Digital Signal Processing Laboratory**, **Control System Laboratory** and **VLSI Laboratory**. The SOP aims to ensure **electrical safety, data security, cybersecurity, and safe working conditions**, while maintaining the integrity of institutional IT infrastructure and simulation environments.

---

2. Scope

This SOP applies to all users of the Electronic Circuits Simulation Laboratory, including those working with:

- Desktop PCs and workstations
- Servers and network storage
- Simulation and design software (e.g., MATLAB, SPICE, HFSS, CST, COMSOL, etc.)
- Laboratory network, printers, and peripherals
- Power strips, UPS systems, and network equipment

This SOP is mandatory for all students, faculty, researchers, and visitors using the laboratory facilities.

---

3. Responsibilities

3.1 Laboratory In-Charge / Faculty

- Ensure compliance with institutional IT and cybersecurity norms (e.g., BUET IT norms).
- Approve any installation of software or connection of external devices.
- Monitor proper usage of computers and network resources.

Prepared By:
Prof. Dr. S. M. Mahbubur Rahman, Dr. Md. Irfan Khan and Mr. Iftekharul Islam Emon

3.2 Laboratory Instructor / Teaching Assistant / Staff

- Ensure users back up important simulation data to network storage.
- Report hardware, software, or network faults promptly.
- Maintain safe electrical installations and adequate ventilation for PCs and servers.
- Ensure regular maintenance of lab computers and network systems.

3.3 Students / Users

- Follow all SOP and Cybersecurity requirements.
- Use laboratory computers only for authorized academic purposes.
- Immediately report hazards, malfunctions, or suspicious activity.

---

4. General Laboratory Safety Rules

- Eating and drinking are strictly prohibited near computers and servers.
- Keep desks, floors, and cable areas tidy to avoid tripping hazards and accidental disconnections.
- Personal chargers and extra devices must not be connected to lab power strips.
- Users must keep their login credentials secure and must log out after use.

---

5. Electrical and Fire Safety Procedures

1. **Ensure Adequate Ventilation**
   Maintain proper airflow around PCs, servers, and UPS units to prevent overheating. Do not block ventilation grills or exhaust fans.
2. **No Wet Hands Near Electrical Equipment**
   Do not touch power sockets, plugs, or cables with wet hands. Any loose, exposed, or damaged power cords must be reported immediately.
3. **Prevent Overloading of Power Strips**
   Do not connect personal chargers or additional devices to lab power strips. Overloaded outlets can cause overheating and fire hazards.
4. **Report Electrical Hazards Immediately**
   If sparking, burning smell, smoke, or overheating is observed, stop work immediately and inform the lab supervisor. Disconnect power only if it is safe to do so.
5. **Electrical Safety Measures**
   Keeping benches clean and dry, reporting damaged cables, and organizing cables reduce electrical hazards and accidents.

Prepared By:
Prof. Dr. S. M. Mahbubur Rahman, Dr. Md. Irfan Khan and Mr. Iftekharul Islam Emon

6. **Cybersecurity Compliance**
   Following BUET IT norms ensures cybersecurity, system stability, and protects against unauthorized access. (2 factor authentication)

---

6. BUET IT Norms

1. **Acceptable Use of IT Resources:** University internet, email, servers, and computer systems must be used only for academic, research, and official purposes.
2. **User Authentication and Account Security:** Users are responsible for protecting passwords, avoiding account sharing, and maintaining secure access credentials.
3. **Internet and Wi-Fi Access Rules:** Access to the campus network and Wi-Fi is restricted to authorized students, faculty, staff, and approved guests.
4. **Prohibited Activities:** Hacking, unauthorized access, spreading malware, piracy, illegal downloads, and misuse of university IT systems are strictly prohibited.
5. **Software Licensing Compliance:** Only legally licensed and approved software may be installed or used on university-owned devices and networks.
6. **Email Usage Policy:** Official university email accounts must be used responsibly and should not be used for spam, harassment, or unauthorized mass communication.
7. **Data Privacy and Confidentiality:** Users must protect sensitive academic, research, and administrative data from unauthorized disclosure.
8. **Monitoring and Network Audit:** The university reserves the right to monitor network traffic, system usage, and security logs to ensure compliance and cybersecurity.
9. **Use of Personal Devices:** Personal laptops, smartphones, and storage devices connected to the university network must comply with security requirements**.**
10. **Do Not Modify System or Network Settings:** Users must not change OS settings, firewall rules, antivirus configurations, or network settings on lab computers.
11. **Social Media Usage Policy:** The use of social media is strictly prohibited inside the laboratories. Disciplinary action may be taken against anyone involved in posting laboratory pictures or videos on social media, or engaging in any form of cyberbullying related to laboratory activities.

---

7. Data Management and Backup Procedures

1. **Regular Data Backup**
   Back up simulation files and project data regularly to authorized network storage or approved institutional cloud services.
2. **Do Not Store Sensitive Data Locally**
   Avoid storing critical data only on local PCs. Local storage may be cleared periodically for maintenance.

Prepared By:
Prof. Dr. S. M. Mahbubur Rahman, Dr. Md. Irfan Khan and Mr. Iftekharul Islam Emon

3. **Protect Data Integrity**
   Do not install cracked software, unauthorized plugins, or scripts that could compromise system stability or data integrity.

---

8. Workspace Safety

1. **Manage Cables and Walkways**
   Avoid tangled cables under desks. Keep floors clear to prevent tripping and accidental pulling of systems or monitors.
2. **Maintain Proper Seating and Posture**
   Adjust chairs and monitors to avoid strain during long simulation sessions.
3. **Keep Workstations Organized**
   Place peripherals neatly to avoid cable strain and connector damage.

---

9. Standard Operating Workflow

Before Use

- Check that ventilation paths are clear.
- Ensure no liquids are present near the workstation.
- Log in using your authorized credentials only.

During Use

- Save and back up simulation data regularly.
- Do not connect personal USB devices or chargers.
- Do not alter system or network settings.
- Monitor for overheating or unusual noises.

After Use

- Log out of your account properly.
- Close applications and save data to network storage.
- Keep the workstation tidy and cables organized.
- Report any issues observed during the session.

Prepared By:
Prof. Dr. S. M. Mahbubur Rahman, Dr. Md. Irfan Khan and Mr. Iftekharul Islam Emon

10. Incident and Emergency Procedures

- **Electrical Hazard / Fire Risk:** Stop work immediately and inform the lab supervisor. Follow institutional emergency protocols.
- **System Malfunction / Malware Suspicion:** Disconnect from the network if instructed and report to IT support.
- **Data Loss:** Inform the instructor or lab technician immediately to attempt recovery from backups.
- **Incident report guidelines:** If any equipment gets damaged while using it, make an incident report and submit to the lab in-charge

---

11. Training and Compliance

- All users must attend a Computer Lab Safety briefing before using the facility.
- Violation of SOP or IT norms may result in suspension of lab access.

Prepared By:
Prof. Dr. S. M. Mahbubur Rahman, Dr. Md. Irfan Khan and Mr. Iftekharul Islam Emon