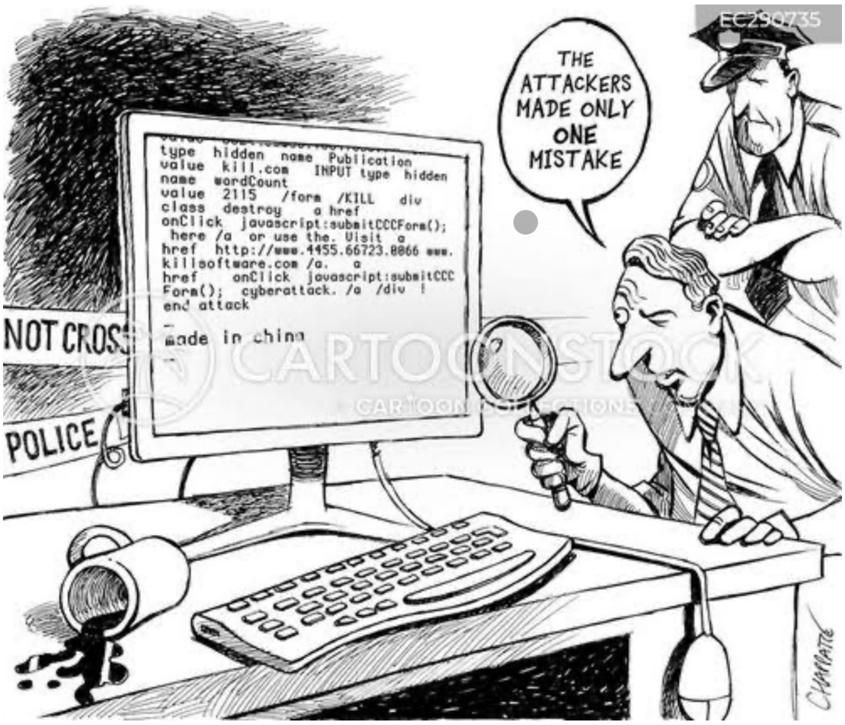
IQAC, GOVERNMENT P.G. COLLEGE, NEW TEHRI, TEHRI GARHWAL – 6 June 2024

Standard Operating Procedures (SOP) for the utilisation & security of information communication technology tools

खलः करोति दुर्वृत्तं नूनं फलति साधुषु । दशाननोऽहरत् सीतां बन्धनं च महोदधेः ॥

“The evil man commits a crime. The punishment could fall upon the virtuous man. As an example, King RAVANA kidnapped Princess SEETA, but who got hurt by the building of an earthen bridge? The ocean, who had nothing to do with the crime.

Standard Operating Procedure (SPO) for the utilisation and security of ICT tools in the college premises


THE ATTACKERS MADE ONLY ONE MISTAKE
type hidden name Publication
value kill.com INPUT type hidden
name wordCount
value 2115 /form /KILL div
class destroy a href
onClick javascript:submitCCCForm();
here /a or use the. Visit a
href http://www.4455.66723.8866 www.
killsoftware.com /a. a
href onClick javascript:submitCCC
Form(); cyberattack. /a /div !
end attack
made in china
NOT CROSS
POLICE
EC290735

Source: https://www.cartoonstock.com/directory/c/cyber_ethics.asp

○**INSPIRATION:** In compliance with the office memorandum "***No. 22001/ 09/ 2023- CP***", Dated 08.01.2024, of the Government of India, Ministry of Home Affairs, Cyber and Information Security Division the IQAC of the Government P.G. College, New Tehri, T.G., is directed to outline a set of rules (SOP) for the utilisation and security of ICT tools, in the welfare of all the stakeholders of the Institution

A. PURPOSE

This SOP aims to ensure the secure, effective & ethical utilisation of the information and communication technology (ICT) tools in the college premises.

B. SCOPE

This SOP applies to all the stakeholders of the Institution, namely employees, students and visitors, who utilise the organisation's ICT tools.

C. DEFINITIONS

ICT Tools: Includes smart boards, LCD panels, computers, laptops, tablets, CCTVs, mobile phones, network devices, printers, scanners, networking hubs, internet/ intranet services etc. of the institution.

Stakeholder: Any member or visitor of the organisation using ICT tools of the institution.

D. RESPONSIBILITIES

- **WebSite Committee & ICT Committee** of the College shall be responsible for the installation, maintenance, and security of all the ICT tools.

- **Stakeholders/ Users**: Shall be responsible for the proper and secure use of ICT tools.

E. PROCEDURES

-Usage of Tools

1. Authorised Use: Only authorised personnel are allowed to use ICT tools.

2. Software Installation and updation: New software and updation to the ICT tools can only be installed with the permission of the **Head of the Institution, WebSite Committee & ICT Committee of the college**.

3. Data Backup: Regular backups of important data must be performed.

-Security Measures

1. **Password Protection:** All ICT tools must be protected with strong passwords, which should be changed regularly.

2. **Antivirus and Anti-Malware:** Ensure all devices have updated antivirus and anti-malware software installed.

3. **Network Security:** Secure all network connections, including Wi-Fi, with strong encryption and regularly update network security settings.

4. **Access Control:** Implement role-based access control to ensure users only have access to the data and systems necessary for their roles.

5. **Physical Security:** Protect ICT tools from physical threats, such as theft or damage, by securing devices in locked rooms or using security cables.

6. **Encryption:** Use encryption for sensitive data, both in transit and at rest, to prevent unauthorised access.

7. I**ncident Reporting:** Immediately report any security incidents, breaches, or suspicious activities to the **Head of the Institution, WebSite Committee & ICT Committee of the college**.

8. **Regular Audits:** Conduct regular security audits and vulnerability assessments to identify and mitigate potential risks.

9. **Training:** Provide regular training sessions for all the stakeholders/ users on the best practices for ICT security and proper tool utilisation.

-Compliance

Non-compliance with this SOP may result in disciplinary action and potential legal consequences. Stakeholders/ Users are expected to adhere strictly to the outlined procedures to ensure the security and effective utilisation of ICT tools.

-Review and Updates

This SOP will be reviewed annually and updated as necessary to address emerging threats and technological advancements.

By adhering to this SOP, the organisation can maintain the integrity, confidentiality, and availability of its ICT resources while ensuring their efficient use.

F. SPECIFIC SECURITY MEASURES FOR LED/LCD PANELS, LAPTOPS, DESKTOPS, PRINTERS AND LAN

1. Use only standard account for accessing the computers/ laptops and LED panels. Admin access shall only be given to the users with the approval of Head of Institution.

2. Set up three layer protection by means of passwords, namely BIOS password, Operating system password and screen saver password. More preferably, if the tool supports biometric authentication, go for it.

3. Ensure that Operating system and BIOS firmware are updated with the latest security patches.

4. Ensure that the antivirus/ anti-malware Clint's installed on the systems/ devices are up-to-date.

5. Always let the system/ device in the default updation state, i.e., in auto-update mode.

6. Only prefer those applications/ softwares, which are listed in authentic and authorised app stores. Never allow third party apps/ software for your system.

7. Allow the system to remain in lock/ log off mode, when not in use.

8. Shutdown/power off the system before leaving the ICT facilitation centre of the college.

9. Set up unique password for shared devices such as printer, scanner Etc.

10. Never allow unauthenticated network services to the printers.

11. Always configure the printer to disallow storing the printing history.

12. Keep the sensors (viz. Wi-Fi, Bluetooth, NFC, GPS, camera) of the desktop/ laptop, while not in use.

13. Keep regular backup of critical data.

14. Never share hard disk data or folder with anyone.

G. INTERNET BROWSING SECURITY MEASURES

1. Always use authentic browsers (e.g., internet explorer, Google chrome, safari etc.) for exploring internet services.

2. While accessing Government services/ applications, email services, or banking/ payment related services, prefer private browsing/ incognito mode in your browser.

3. While accessing the sites and services, where login is required, always use to type the site address/URL/ link manually on the browser's address bar rather than clicking on any link.

4. Do not unnecessarily allow cookies/ fishing sites during the browsing.

5. Never allow your browser to store/remember your login credentials.

6. Never allow your browser to store any finance/ payment related information.

7. Don’t allow any third party service provider to control your system. Also, avoid using unauthorised VPN services and Remote Desktop tools like Any-desk and TeamViewer.

8. Never download any unauthorised or pirated content/ software from the internet.

9. Never install or play games on your official computer.

10. Develop habit of clearing cache memory and browsing history.

11. Enable genuine ad-blockers and firewalls to avoid malware and bloat wares

H. MOBILE SECURITY MEASURES

1. Make sure that your mobile is running on the updated and latest operating system.

2. Never root or jailbreak your mobile device. Jail breaking disables many in-built security aspects of the device.

3. Always keep the sensors (GPS, Bluetooth, Hotspot, NFC, IR blaster etc.) off, while not in use.

4. Download Apps from the official stores of Google (for Android) and Apple (for IOS). Do not install any third party app in your mobile from untrusted sources.

5. While participating in college meetings, sensitive discussion, academic discussion, lectures in classes, always switch-off your mobile, or leave the mobile outside the meeting/class room.

6. Don’t accept any unknown Bluetooth pairing request or file sharing request.

7. Be aware of the the permissions required by any App installed in your mobile phone.

8. Note down the unique 15-digits IMEI number of your device and keep it offline. It will be useful in case of any physical loss of device.

9. To avoid unauthorised access to your device, keep your device in auto lock mode by means of patter and biometric passcode process.

10. Always use the feature ‘mobile tracking’ enable

11. Backup your phone's storage at regular intervals.

12. Always use a genuine anti-malware/ anti-virus software as a security companion to your mobile device.

13. Report the lost or stolen device immediately to the nearest police station and the concerned service provider.

14. Always keep your device disable to the automatic downloads

I. E-MAIL SECURITY MEASURES

1. For your official mail, ensure that the KAVACH APP for multi-level authentic is installed to your device.

2. Do not share the e-mail password and OTP with unknown/ unauthorised person.

3. Don't use any unauthorised/ external email service for official communication.

4. Never Leave the device logged in with your email address.

5. Don't click/ open the attachments send by unknown senders.

6. Be cautious about the current social engineering attacks and do not install apps/files in your computers based on direction/instructions over mobile phone.

J. SOCIAL MEDIA SECURITY MEASURES

1. Restrict yourself to expose your personal information while accessing social media and networking sites.

2. Always check the authenticity of the person, while accepting request as friend/ contact.

3. Use multi-factor authentication to secure the social media account.

4. Develop the habit of changing passcodes for your social media account at regular intervals.

5. Do not click the attachment/ links sent by unknown senders.

6. Do not publish/post/share any Government document or information at social media platforms.

7. Do not publish/ post/ share any unverified information at social media platforms.

8. Do not share any official document through messaging apps like WhatsApp, Telegram, Signal etc. For sending/sharing official document, it is recommended to use SANDESH APP of NIC to share official document.

9. Avoid to share any private information, such as home address, mobile, contact numbers, UID, PAN on social media platforms.

10. Maintain social media privacy setting at secure level.

11. Avoid the Ads, that promise free money, prizes any any kind of discount.

K. ONLINE VIDEO CALLS AND CONFERENCING SECURITY MEASURES

1. Enable the password authentication to participate in the conference room.

2. Enable waiting room feature in video conferencing App/ Software.

3. Enable lock meeting feature when all the participants have joined.

4. Disable camera, microphones, screen sharing, and remote monitoring functionalities until requested.

5. Turn off anything that gives too many permission/access to the meeting App.

L. INTERNET CONNECTION SECURITY MEASURES

1. Enable strong and updated secure encryption in wireless networks.

2. Make necessary changes in default credentials for wireless Admin.

3. Wireless router firmware should be updated at regular intervals.

4. Disable remote management functionalities like WPS and universal plug and play.

5. Turn on MAC address filtering and MAC binding to decline the access sought by unauthorised devices.

6. Avoid connecting your personal devices to the unprotected unsecured networks.

7. Keep wireless network down, when not in use.

M. SECURITY ADVISORY AND INCIDENT REPORTING

1. Kindly comply the guidelines of the NISPG and other security advisories published from time to time by CERT-In, MHA, NCIIPC, MeiTY and other important government organisations.

2. Report any cyber security incident, including suspicious and phishing mails immediately to CISO-In (incident@cert-in.org.in) and NIC-CERT (incident@nic-cert.nic.in)

N. CYBER SECURITY RESOURCES

SL NO.	Resource URL	Description
1	https://www.meity.gov.in/cyber-security-division	Laws, policies & guidelines
2	https://www.cert-in.org.in	Security advisories, Guidelines & Alerts
3	https://www.csk.gov.in	Security tools & Best Practices
4	https://www.nic-cert.nic.in	Security tools & Best Practices
6	https://cybercrime.gov.in	Report cyber crime and cyber safety tips

O. COMPLIANCE

All the Government Employees, including temporary, contractual/ outsourced, students, and visitors are required to strictly adhere to the guidelines mentioned in the SOP in full letter and spirit. Any non-compliance may be acted upon by the Head of the Institution.

INFORMATION COMMUNICATION TECHNOLOGY TOOLS AND CYBER ETHICS:

-Preamble: The content outlined herein is intended to create awareness among citizens, especially students and various stakeholders of the Institution about various cyber threats that can impact them and pave the way to safeguard themselves against cyber crimes.

-Ethics: Information and communication technology has become an integral part of our everyday lives. Therefore its our duty to turn ourselves as a responsible and careful cyber citizens of the present and future cyber world.

-**Cyber Crimes**: Cyber crimes are offences that may be committed against individuals, companies, or institutions by using ICT tools , such as computers, mobiles, and other electronic devices. Generally, cyber criminals use platforms such as social networking sites, emails, social media platforms, websites etc. to attack victims.

-Cyber threats that can impact anyone: Cyber threats are various possible ways that can be used by Hacker to attack us using internet or mobile technology.

-Some common ways used by cyber criminals:

- **Email Spoofing**-Sending out an e-mail to you that look like genuine
- **Malicious files applications-** Sending you malicious and bad applications and files through direct messaging, gaming, emails or websites etc.
- **Social engineering-** a technique used by cyber criminals to gain your confidence to get information from you.
- **Cyber bullying-** A form of harassment or bullying using electronic or communication devices.
- **Identity Theft-** Using someone's ID mischievously to gain financial benefits.
- **Job Frauds-** Deceptive activity on the part of an employee towards an employer.
- **Banking Frauds-** Fraudulently obtaining money from depositors.

REFERENCE(S):

1. office memorandum "***No. 22001/ 09/ 2023- CP***", Dated 08.01.2024, of the Government of India, Ministry of Home Affairs, Cyber and Information Security Division
2. A handbook for adolescents/ students on cyber safety: Ministry of Home Affairs, Government of India.