Central University of Haryana

ICT Section

Cyber Awareness and Cyber Hygiene Guidelines

1. General Cyber Hygiene Practices

- Keep your mobile and computer operating systems, antivirus software, and applications regularly updated.
- Use strong, unique passwords and enable multi-factor authentication (MFA).
- Backup critical data periodically on secure, offline or cloud storage.
- Use official email and communication channels for institutional work.
- Ensure devices are locked when unattended.
- Connect only to secure Wi-Fi networks.
- Regularly review and manage application permissions and data-sharing settings.

2. Cyber Awareness – Do's and Don'ts

Do's

- ✅ Verify the sender's identity before opening attachments or clicking links.
- ✅ Report suspicious emails or cyber incidents to the IT/Security Cell immediately.
- ✅ Use official institutional credentials for academic and administrative portals.
- ✅ Use **strong passwords** – at least 12 characters with letters, numbers, and symbols.
- ✅ Log out of accounts when using shared or public computers.
- ✅ Educate peers and colleagues on safe online habits.
- ✅ Attend institutional workshops and awareness programmes regularly.
- ✅ Follow updates from **Ministry of Electronics & IT (MeitY)**, **CERT-In**, and **UGC** for latest advisories.

Don'ts

- ❌ Don't share passwords, OTPs, or confidential data with anyone.
- ❌ Don't use pirated or unlicensed software.
- ❌ Don't click on unknown or suspicious links/pop-ups.
- ❌ Don't connect personal USB devices or drives to official systems without scanning.
- ❌ Don't post or forward unverified information on email/social media.
- ❌ Don't ignore system warnings or update prompts.
- ❌ Don't access sensitive institutional data through unsecured networks.

3. Reporting

- In case of cyber incidents, report promptly through:
  - **CUH ICT Helpdesk(ict@cuh.ac.in/01285260250)**
  - **National Cyber Crime Reporting Portal: https://cybercrime.gov.in**

Incharge, ICT Section