DO's and DON'Ts at Office

DOs at Office

- Use only a Standard User (non-administrator) account for regular work on Computer.
- Set a BIOS password for booting.
- Ensure that the Operating System and BIOS firmware are updated with the latest patches.
- Enable automatic updates for the Operating System from trusted sources.
- Keep the antivirus client updated with the latest virus definitions, signatures, and patches.
- Use only applications/software authorized by ICT Section.
- Shut down your desktop before leaving the office.
- Keep printer software updated with the latest patches.
- Set up unique passcodes for shared printers and disable print history storage.
- Enable the desktop firewall to control information access.
- Keep GPS, Bluetooth, NFC, and other sensors disabled on desktops, laptops, and mobile phones unless required.
- Use a hardware VPN token for connecting to IT assets in the Data Centre.
- Use complex passwords (minimum 8 characters) with a mix of uppercase, lowercase, numbers, and special characters.
- Change passwords at least once every 30 days.
- Enable Multi-Factor Authentication (MFA) wherever possible.
- When accessing government, banking, or other critical services, always use Private Browsing/Incognito Mode.
- Always type website URLs manually instead of clicking links from emails or messages.
- Use the latest version of your internet browser and ensure it is regularly updated.
- Be cautious with shortened URLs (e.g., tinyurl.com/...). They may lead to phishing or malware sites.
- Keep your mobile operating system updated with the latest patches.
- Keep Wi-Fi, GPS, Bluetooth, and NFC disabled on mobile phones unless needed.

- Download apps only from official app stores (Google Play for Android, App Store for iOS).
- Review app permissions and user feedback before downloading any application.
- Switch off or leave your mobile device outside during sensitive discussions.
- Record your device's unique 15-digit IMEI number and store it offline for loss reporting.
- Enable auto-lock and use secure passcodes or patterns on mobile devices.
- Enable mobile tracking and configure trusted contact numbers for recovery in case of theft.
- Take regular offline backups of your phone and memory cards.
- Scan data with updated antivirus software before transferring it to or from a mobile device.
- Be cautious when opening links shared via SMS or social media — avoid suspicious offers or news links.
- Report lost or stolen devices immediately to the police and your service provider.
- Disable automatic downloads on your phone.
- Keep antivirus software updated and active at all times.
- Ensure that Kavach Multi-Factor Authentication is configured for your NIC email account.
- Download the Kavach app only from official app stores.
- Use PGP or a digital certificate to encrypt sensitive emails.
- Disable macros when opening downloaded attachments and keep 'Protected Mode' enabled in MS Office.
- Perform a low-level format of removable media before first use and scan with antivirus software.
- Encrypt files and folders on removable media and protect important documents with strong passwords.
- Limit sharing of personal information on social media and verify contacts before accepting requests.
- Use Multi-Factor Authentication for securing social media accounts.
- Regularly review your CUH email login history and report any suspicious activity to ICT Section.

DON’Ts at Office

- Don’t store usernames or passwords in internet browsers.
- Don’t save payment-related information in browsers.
- Avoid using third-party anonymization services (e.g., NordVPN, ExpressVPN, Tor).
- Don’t install unauthorized browser toolbars or extensions.
- Avoid downloading unauthorized or pirated content (e.g., movies, music, software).
- Don’t install or play games on official systems.
- Never reuse passwords across multiple accounts or services.
- Don’t write down or display passwords, IPs, or network details on unsecured materials (e.g., sticky notes).
- Never share system passwords, printer passcodes, or Wi-Fi credentials with unauthorized persons.
- Use only authorized software approved by ICT Section.
- Always lock or log off your desktop when not in use.
- Disable internet access to printers.
- Don’t use mobile app-based scanners (e.g., CamScanner) for internal documents.
- Delete any pirated or unauthorized operating systems and software immediately.
- Don’t root or jailbreak mobile devices as it disables built-in security features.
- Don’t accept unknown Bluetooth pairing or file-sharing requests.
- Never share email passwords or Kavach OTPs with unauthorized persons.
- Use only official email accounts for official communication.
- Avoid clicking links or opening attachments from unknown senders.
- Don’t plug removable media into unauthorized devices.
- Never post or share internal government documents or information on social media.
- Avoid posting unverified information on social platforms.

- Don’t share your @cuh.ac.in, @gov.in or @nic.in email address on social media.

- Avoid installing apps that request excessive permissions unrelated to their function (e.g., calculator app requesting GPS).