Information Security is the shared responsibility of every CyberTech employee. You play a key role in safeguarding confidential information and organizational resources. Below are the Do's and Don'ts as per CyberTech's Information Security Policy-

- We use Microsoft Active Directory for access, authentication, and authorization. CyberTech has defined corporate security and password policy for Microsoft Active Directory. Create strong and difficult-to-guess passwords. As per the policy, ensure that your password consists of a minimum of 8 characters, including uppercase letters, lowercase letters, numbers, and special characters.

- Use different passwords for different corporate resources (such as Salesforce, SuccessFactors, etc.) to prevent compromising multiple accounts if one password gets hacked. Please change the password every month.

- Keep your passwords confidential - DO NOT share them with others or write them down. You are solely responsible for all activities associated with your credentials.

- Use only CyberTech-authorized means of communication such as CyberTech email, Teams, Salesforce, etc. Refrain from using unauthorized mediums such as WhatsApp, iMessage, LinkedIn, Gmail, Facebook, etc. for official communications. These social media tools are a big source of Cybersecurity threats.

- Lock your computer and mobile phone when not in use to prevent unauthorized access and use of data.

- Do not leave sensitive information unattended in the office. Refrain from leaving printouts or portable media containing sensitive/private information on your desk. Instead, lock them in a drawer to minimize the risk of unauthorized disclosure.

- Refrain from posting private or sensitive information, including passwords, or any other personal details, on public sites and social media platforms. Additionally, do not send such information via email.

- Be vigilant of phishing traps in emails and be attentive to tell-tale signs of scams asking for money or information. If you receive a suspicious email, immediately delete the message, report it to your manager, and inform the DEIT representative.

- Do not click on links from unknown or untrusted sources. Cyber attackers often employ deceptive tactics to lure individuals into visiting malicious websites or downloading malware that can compromise data and networks.

- Use encryption to protect sensitive data being transmitted over the internet.

- Do not use Public Wi-Fi hotspots on corporate devices. Public wireless networks are inherently insecure.

- Do not fall for attempts to extract confidential information. Unauthorized individuals may impersonate employees or business partners through phone calls or emails. Do not respond to requests for confidential data. When in doubt, verify the authenticity of the request with your CyberTech DEIT support staff.

- Phishing scams target the general population of our employees while spear phishing targets a specific particular individual in CyberTech. Be extremely watchful of these unauthorized solicitations.

- Whaling attack doubles down on sphere phishing. It not only targets key individuals; but also in a way that the fraudulent communications appear to have come from someone specifically influential in the organization. Think of them as "big phish" or "whales" at the company, such as the CEO or CFO. This adds an extra element of social engineering, with staff reluctant to refuse a request from someone they deem to be important. Our corporate officers will never send emails or WhatsApp requests for assistance.

- Properly dispose-off the information when it is no longer needed. For electronic storage media, consult with the IT department for appropriate disposal methods by returning to DEIT.

- Be aware of your surroundings when handling sensitive information while printing, copying, or discussing it. Collect printed materials from printers promptly.

- Do not install unauthorized programs on your work computer. Malicious applications often masquerade as legitimate software. Contact your DEIT support staff to confirm whether an application may be installed.

- Do not connect portable devices to your work computer without permission from the DEIT team. These devices may contain compromised code that could launch as soon as they are plugged in.

- Avoid leaving devices unattended and ensure the physical security of all mobile devices, including laptops and cell phones. In case of loss or theft, report the incident immediately to your manager and the DEIT representative.

- Keep areas containing sensitive information physically secured and grant access only to authorized individuals. Safeguarding CyberTech data and preventing its damage, loss, or theft is your responsibility.

- Refrain from keeping any local copies of source code and sensitive corporate data. Storing data solely on secure servers or designated repositories minimizes the risk of unauthorized access or loss.

- Take regular backups of critical data and store them on OneDrive. Regular backups help prevent data loss in the event of hardware failure, accidental deletion, or a security breach.

- Refrain from keeping any personal data within corporate assets. Personal data includes sensitive information such as personal identification numbers, financial details, or any other personally identifiable information.

- Be accountable for the corporate information you hold and the assets assigned to you.

- Report all suspicious activity and cyber incidents to your manager and the DEIT representative.

- Understand your responsibilities with CyberTech's IT Resources Usage Policy & follow CyberTech's Information Security Policies and related standards.

CyberTech's Information Security Management Team is dedicated to ensuring the protection of privacy, safeguarding of CyberTech's information assets and infrastructure, identification and mitigation of vulnerabilities, detection, response, and recovery from cyber incidents, as well as promoting cyber awareness and education within the organization. Our dedicated Information Security Management Team is committed to assisting and supporting you in your cyber security risk management endeavours.

Information also needs to be protected from theft, loss, damage, leakage, etc. We all need to follow Information Security dos and don'ts for Confidentiality, Integrity, and Availability of information.

Remember - Cyber Security is Everyone's Responsibility!

Read & Understood

Name: A BRIJESH

Date: 06/02/2025

Contact DEIT Team on **Phone +91 9167469445** and **Email deit@cybertech.com** for and questions or to report any incident.

CyberTech Systems and Software Limited
CyberTech House, B - 63/64/65, MIDC Wagle Estate, J. B. Sawant Marg Thane, Maharashtra, 400604 India