Cyber Security Centre of Excellence
West Bengal

Department of Information Technology & Electronics
Government of West Bengal

General IT security advisory

Domain: Server
Dos

1. Ensure that the Operating system(OS)s are installed with the latest OS updates/patches.
2. Ensure that Antivirus Clients are installed on all machines. Full System scan should be done at least once in a week and Quick/Flash scans should be done at least once in a day.
3. Ensure that all Database servers, web servers, etc. are appropriately hardened.
4. Ensure that only the necessary ports and protocols are opened in the servers for communication.
5. Ensure that logging is enabled in all servers, security devices, storage, Virtual Machine (VM)s and any other ICT Infrastructure or Services, where logging is supported.
6. Always download updates and patches from the Official websites or Repositories of the respective Original Equipment Manufacturer.
7. Ensure that all the sites and applications are using https (i.e., valid SSL certificate).
8. Ensure that data is backed up under a given policy for Application and Database.
9. Ensure sensitive information on the computer screen is not visible to others.
10. Protect sensitive files and devices with appropriate password.

Don'ts

1. Use the Root Account or Super User or Administrator Account in your servers, for day to day activities.
2. Install any pirated software or cracks on your machines.
3. Use the same credentials on multiple machines.
4. Leave your computer / sensitive documents unlocked.
5. Plug in personal devices without an "OK" from the competent authority.

Domain: Desktop/Laptop
Dos

1. Ensure that Antivirus Clients are installed on all Client machines.
2. Ensure that full System scan should be done at least once in a week and Quick/Flash scans should be done at least once in a day.
3. Ensure that security hardening is carried out in all client machines.
4. Especially users who login to with admin credentials through VPN must ensure that they have updated their laptops / desktops with latest patches.
5. Ensure sensitive information on the computer screen is not visible to others.
6. Protect sensitive files and devices with appropriate password.

    Webel Bhavan, Ground Floor, Block - EP & GP, Sector – V, Bidhannagar, Salt Lake, Kolkata - 700 091

Don'ts

1. Don't install any pirated software or cracks on your Client machines.
2. Don't store sensitive information in portable device without strong encryption.
3. Don't leave your computer / sensitive documents unlocked.
4. Don't plug in personal devices without the OK from IT.

Domain: Application
Dos

1. Ensure that all Open Source or Proprietary - Applications, Frameworks, Software, Packages, Integrated Development Environments (DBMS), Data Base Management System(DBMS), Reporting/Business Intelligence/Analytical Tools, Services, Application Programming Interfaces(API), Components, Libraries, Plugins etc., used on both the server and client machines do carry the latest updates/patches.
2. Ensure that logging is enabled in all servers, web servers, Content Management Systems(CMS), DBMS, network devices, security devices, storage, VMs and any other ICT Infrastructure or Services, wherever it is supported to track any malfunction.
3. Always download updates and patches from the Official website or Repositories of the OEM.
4. On a daily basis check all files present under the Website root directory and Upload directory for any unauthorized file modifications and deletions.
5. Ensure that all API Calls are done through encrypted channel.
6. Ensure that all credentials, API Keys, connection strings are encrypted.

Domain: Network
Dos

1. Ensure that all the sites and applications are using https (i.e., valid SSL certificate).
2. Make sure your Internet connection is Secure.
3. Use segmented networks for optimal performance and security.
4. Keep the switch ports (physical) blocked when not in use.
5. Avoid using vulnerable activities over your network.