Infosys Limited Information Security Do's and Don'ts Policy

This Information Security Do's and Don'ts policy applies to all subcontractors who do not have logical access to the Infosys network, including their agents, sub-contractors, employees, etc.

The concerned individual shall:

Adherence to policies and processes

1. Abide by all information security and IT infrastructure related policies of Infosys, Infosys clients published in ISG portal or communicated via different channels like email, Do's & Don'ts, awareness mailers, etc.
2. Remember that any violation of Infosys' or Infosys client (the customer of Infosys that you are supporting on behalf of Infosys) policies could lead to disciplinary action including but not limited to immediate revocation of access to the concerned systems, suspension from employment and termination from employment.

Physical security and access control

3. Follow the physical security processes of the company. The individual must always wear his/ her/ their Client badge when he/ she/ they are inside the office.
4. Report any physical security incident to the security guards or admin staff nearest to them.
5. not attempt to enter/access areas where he/ she/ they are not authorized to enter. Even at authorized areas, the individual must ensure that he/ she/ they enter only after he/ she/ they have swiped their access card. Tailgating is not permitted.

Password best practices

6. Be aware of the Infosys and Client password policy. Never disclose your passwords, even to your manager, team members or even to an auditor.

Data privacy

7. Use due care and diligence while accessing, processing and using personal data. The individual must not share the same with anyone other than those that have a business need to know.

8. not use any copyrighted/patented material without the required authorizations and approvals in place.
9. Beware of phishing emails and other fraudulent methods used by hackers like social engineering (the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes), etc.
10. Do not share any Personally Identifiable Information/ sensitive data (Including, but not limited to email id, contact number, health information, financial information etc.) of any individual, including Infosys employee(s) /third parties/Infosys customers with any unauthorized recipients and/ or without the express consent of the concerned individual(s).
11. Do not give out statements to the press about Infosys and related matters. All queries must be directed to Infosys' public relations officer <PR_Global@infosys.com>.

Data security

12. Refrain from discussing Infosys or Client information in public, posting related information on social networking sites such as LinkedIn, or uploading code etc. to external websites and forums.
13. Classify all data as per sensitivity and adopt appropriate protection measures based on the sensitivity of the information.
14. not keep any sensitive printed information unattended on his/ her/ their desk or the printer. Use a shredder to securely destroy sensitive printed information after its perusal
15. Return all project related material and information at the time of your release. Having access to the earlier project's data, while you have moved to a new project, is not recommended.
16. Safeguard the Infosys and Client assets allocated to the individual, including laptop, smartphone, secure ID token etc. from theft and accidental loss. Ensure that the laptop is encrypted. The individual must notify their manager, immediately in case of loss, so that the required steps can be taken to protect the data.
17. Follow the secure coding practices applicable to the project.
18. Do not disable the security solutions like anti-virus etc. on your computer as this will render it vulnerable.
19. Lock the screen of your computer when unattended.

Email and Internet usage

20. Do not send sensitive information belonging to Infosys or Client, outside Infosys/Client networks. Sending information to personal email addresses is not permitted.
21. Use your Infosys/Client email ID only for official purposes and must not share the same in online forms/forums etc.
22. not forward chain mails to other employees. All spam mails must be immediately reported to Infosys IT team at icert@infosys.com. The individual must refrain from opening non-business related attachments (e.g. games) even if it is from a trusted sender
23. Use internet responsibly and avoid illegal and objectionable practices while using the internet at work e.g. browsing malicious sites, accessing blocked sites using proxy avoidance techniques etc.

Software licensing and usage

24. Always use software that is licensed for use at Infosys. Do not violate the licensing terms and conditions and download unauthorized software even if it is for a business critical need
25. Refrain from using P2P software and sharing folders.

Business continuity and Disaster recovery

26. Always store critical project related information and official Outlook PSTs on the server as this will ensure that it is regularly backed up by CCD.
27. Be aware of the emergency exits of your floor and the safe assembly points to use in case of a disaster. Know the Disaster Recovery Representatives (DRR) on your floor, who would assist you in case of any emergency.
28. Diligently participate in the fire and evacuation drills that take place in the Development Centre (DC)/ client location on a regular basis.
29. Be aware and store the emergency helpline numbers of your DC.

Security Incidents

30. Immediately notify your manager to report any actual or potential security incidents that may result in a data security breach for Infosys. For Client related incidents please be aware of the Client notification process to whom you need to contact in case of any incident.