Click here to Go Back to Index Page

User Responsibility for Information Security

User Responsibility Check List (Clean Desk Policy included)

1	√ Are you aware of, and understand **latest version of Information Security Policy** of the organization ?
2	√ Have you read, understood and signed off the **Employment Agreement, Code of Conduct & Discipline, with reference to applicable Role** (or Job description) and associated Information Security Risk Rating with organization, and with its customers if it is required as part of agreement?
3	√ Have you gone through appropriate **Pre-Employment Screening** requirement with reference to your Role in organization and associated Information Risk Rating with it?
4	√ Are you aware that anytime during employment, you must **disclose any conflict of interest** which could be potential risk to organization?
5	√ Have you read, understood and signed off the **Confidentiality Agreement (Non-Disclosure Agreement)** with organization, and if work with your customers require any specific obligation of the type ? Do you have a copy of these documents for your continued awareness?
6	√ Are you aware of **Information Security Structure** in organization, and whom to **contact in case Incident occurs** or it gets into your notice?
7	√ Are you aware that information asset, identity card, password, keys, data devices and **Information processing facility given in your custody** are your responsibility, and any loss of it is a security incident, and it needs to be reported at once?
8	√ Are you aware that **no hardware or/and software can be brought into premise** of this organization or introduced into its information processing facility without written approval of Head of Organization ?
9	√ Are you aware that **no private data can be kept in Information Processing facility of organization** or with equipments in your custody for work?
10	√ Are you aware that you are **not allowed to share passwords, identity card, keys, data devices, and information processing equipment** given in your custody to anyone else? If others share such a thing, bring it to knowledge of Information Security Incharge at once?
11	√ Are you aware that **unauthorized copying of files or document is not allowed** and if it is a work requirement, any such copy or transfer of document is uniquely identified, and must have evidence of delivery?
12	√ Are you aware that any **inadvertent loss of document, data device including in trash or waste papers left unattended at photo copier/ printer and, insecure drawer or desktop** or papers lying loose are information security breach?
13	√ Are you aware that **documents in trash or waste papers left over at photo copier/ printer must be shredded,** and remain unfit for reconstruction ?

14 √ Are you aware that data devices or **information processing equipment cannot be given for repair to any unauthorized agency** or with those without approval/ knowledge of management? In case of need of replacing of existing equipment, data in it must be removed from it, and separately stored.

15 √ Are you aware of the maximum period when you must get **backup of your local data** onto the server of the organization? If this back up is not taken within a period, none would know amount of loss of data, and it is a security incident. Do you know and can show it how can you retrieve that backup data?

16 √ Are you aware of your responsibility of ensuring at least each day that clock of your information processing equipment is **synchronized with date and time of the location**? If this is incorrect, the time and date stamp of document creation, any calendar application and any tracking of access record (from/to) shall be incorrect.

17 √ Are you aware of your responsibility of **ensuring virus scan at least once in a day, key holding responsibility, any restriction on use of mobile device, restriction on use of internet, any other data exchanges, and e-mail** in view of ISMS policy and and legally enforceable nondisclosure agreement with the organization?

18 √ Are you aware of strength of password, complexity and auto-screen lock, and how do you get this policy enforced in settings at your **local self managed information processing facility?**

19 √ Are you aware of **number of seconds that if the computer is passive, it should get automatically locked (after 5 mins) and can be opened by use of this password? Can you show its setting method?**

20 √ Are you aware of **strength of password, complexity and auto-screen lock**, and what is your responsibility with regard to password protection in **a global settings at Server/ Network**?

21 √ Are you aware of the **Email Disclaimer** policy and your responsibility to ensure that any email going out from you business email id should contain this important notice for receivers?