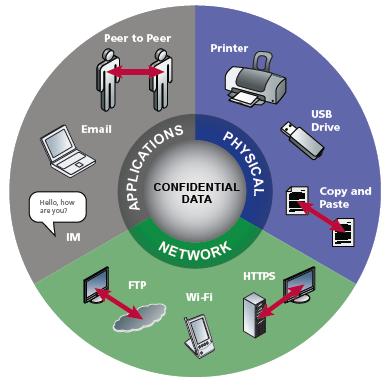
# **TCS has ZERO Tolerance against any Security Violations**

`

* Do not share project related information outside
* Do not share passwords with anyone
* Do not write passwords or any other sensitive information anywhere
* Do not use official email for any non-business purpose
* Do not respond to any suspicious phishing mails received from unknown persons/groups asking for sharing of information, official data or Personal Information.
* Do not upload / download any information using JPMC network from Internet (anything but not limited to Project Plan, Code, Snippet, Employee / Contractor details, confidential documents etc.).
* Do not post technical issues / problems to public forums for any resolution
* Do not share/upload source code to any 3rd party site/blog on the internet or code groups
* Do not send any project/personal documents to TCS email id or any other private email id's using JPMC email id during or while leaving project/account.
* Do not post any information on Client, Project and related information in any social networking sites or on personal messaging apps (SMS, WhatsApp etc.)
* Do not upload or attempt to upload any JPMC material, documents etc. to either TCS Knowmax or any other 3rd party site on the internet.
* Do not visit any unauthorized blogs or BlogSpot's while working in JPMC domain
* Do not misuse JPMC provided resource like internet to do online shopping, gambling, gaming , non-business sites, obscene sites etc. or any other online booking activities using any desktop / laptop
* Do not install any freeware, unauthorized software in the local desktops or JPMC provided laptop / desktop or LVDI / VDI sessions
* Do not use your VDI / LVDI or JPMC provided laptop to download movies, songs or for any personal use
* Do not change any proxy setting or any browser related settings
* Do not use printers or scanners in JPMC (Onsite / Captive) for non-project related requirements
* Do not bring any unwanted media devices like USB, CD, DVD, hard disks etc. inside the ODC
* Do not insert USB or portable device in the desktop/laptop USB port including cellphone USB chargers
* Do not use personal cellphone for accessing JPMC email through any third party application like GOOD
* Read, Understand & Adhere to TCS Security policy and guidelines – Refer to iQMS Wiki site in Ultimatix ([**https://iqmskm.ultimatix.net/km/index.php/IQMS\_longform**](https://iqmskm.ultimatix.net/km/index.php/IQMS_longform) )
* Read, Understand & Adhere to Information security guidelines as published by JPMC – Refer to ***trainingcentral.jpmchase.net***
* Use your own credentials at all times (includes access card, RSA Token, System ID)
* Lock your Desktop/Laptop whenever you leave your desk
* Follow TCS password policy. Use strong, non-dictionary words as your password.
* Follow clean desk, clear screen policy. Keep your workplace neat and clean
* Shred unwanted documents, and destroy unwanted CDs, DVDs, Floppies
* Be aware of social engineers and Social Engineering attempts. Be alert.
* If you get a call from an unknown caller and the caller is demanding any business information, do not share. Be alert and alive to the situation.
* Ensure that the anti-virus is up to date always
* Display your ID card whenever you are at work & Challenge strangers without ID card
* Understand & follow both TCS & Client Security policies and procedures
* Use internet & email only for business purposes(TCS and Customer provided)
* If you receive non-business communication into your client email id please delete it
* Do follow TCS guidelines on document classification
* Collect printouts as soon as you print them

**DON’T’s**

**DO’s**