INFORMATION SECURITY

BEST PRACTICES

General Computer usage – Best practices

- Use account with limited privileges on systems and avoid accessing with administrator privileges for day-to-day usage.
- Keep Operating System, Application software and Anti-Virus software updated by applying the latest service packs and patches.
- Backup of important files at regular intervals.
- Do not leave system unattended. Log out of or lock your computer when stepping away, even for a moment
- Supervise maintenance or rectification of faults in the system by service engineers.
- Do not download unfamiliar software off the Internet.
- Remove unnecessary programs or services from computer: Uninstall any software and services you do not need
- Restrict remote access. If file sharing is not required in your day-to-day work, disable file and print sharing.
- Treat sensitive data very carefully.
- Remove data securely: Remove files or data you no longer need to prevent unauthorized access to them. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system
- If your networking devices are not using IPv6, disable IPv6 from computer.
- Always maintain a redundant power supply.
- Use systems screen locking functionality to protect against physical access, such as a screen saver that wont deactivate without a password, or just log out of everything so anyone that wants access has to log in again.
- Enable the option chassis intrusion in the BIOS settings to be aware of unauthorized users.
- The systems should be placed in a room which is dust free and has a good ventilation to avoid overheating of CPU.
- Do not plug the computer directly to the wall outlet as power surges may damage computer. Instead use a genuine surge protector to plug a computer.
- Don’t eat food or drink near the PC.
- There should be no magnets near to your PC.

- Scan all the files after you download whether from websites or links received from e-mails.
- Download anything only from trust worthy websites. Do not click links to download anything you see on unauthorized sites.
- Don’t click the link or file and let it start download automatically, download the file and save where you want save and then run on the application.
- Never download from the links that offer free antivirus or anti spyware software, always download from trusted sites, if you are not sure about the site you are downloading, enter the site into favourite search engine to see anyone posted or reported that it contains unwanted technologies

General Internet Browsing – Best Practices

- Always use updated anti-virus, Operating System and applications and browser.
- Use a web browser with sandboxing capability (like Google chrome, safari, etc.). Sandboxing usually contains malware during execution.
- Download software from trusted source only.
- Be wary of storing personal information on Internet.
- Do not store any information you want to protect on any device that connects to the Internet.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.
- Make a habit of clearing history from the browser after each logout sessions.
- Delete Windows “Temp” and “Temporary Internet files” regularly.
- Avoid all cloud services (Dropbox, iCloud, Evernote, etc) that are based outside India.
- Avoid using services that require location information.
- Remember search engines track your search history and build profiles on you to serve you personalized results based on your search history.
- Be conscious of what you are clicking on/downloading.
- Some pop-ups have what appears to be a close button, but will actually try to install spyware when you click on it.
- Remember that things on the internet are rarely free. “Free” Screensavers, etc. generally contain Malware.
- Be wary of free downloadable software - There are many sites that offer customized toolbars or other features that appeal to users, which are likely to have backdoors.
- Dont follow email links claiming to offer anti-spyware software - Like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating.
- Frequently check unusual folder locations for document (.doc, docx .xls, .xlsx and .def) file extensions (in search options, select advanced search

options, make sure you checked “Search System folder”, “Search hidden files and folders” and “search subfolders”)

- Avoid Internet access through public Wi-Fi.
- Never exchange home and office work related contents.
- Avoid posting of photos with GPS coordinates.
- Don’t respond to email, instant messages (IM), texts, phone calls, etc., asking you for your password.
- Only click on links from trusted sources. Never click on a mystery link unless you have a way to independently verify that it is safe. This includes tiny URLs.
- Be extremely careful with file sharing software. File sharing opens your computer to the risk of malicious files and attackers. Also, if you share copyrighted files, you risk serious legal consequences.

Malware defense – Best practices

- Always set automatic updates for Operating System, Anti-Virus and Applications. (My Computer -> properties -> automatic updates -> select Automatic and time)
- Enable hidden file & system file view to find any unusual or hidden files. (My computer -> tools -> folder options -> view -> select enabled with “Show hidden file and folders” option and disable “Hide protected operating system files”)
- Turn off auto play (Windows Vista/7 :- Start -> Run -> type gpedit.msc -> Computer Configurations -> Administrative Templates -> Windows Components - > Select “AutoPlay Policies” -> Double Click at “Turn off Auto play” -> Select Enabled -> Set “Turn off Auto play on:” to “All drives” and Click OK.)
- Type: dir %temp% in “run” and delete all entries after opening any suspicious attachments.
- Type cmd in run and type netstat –na. Checkout foreign Established connection and IP addresses. Check the IP address for its ownership.
- Type “msconfig” in “run” and check for any unusual executable running automatically.
- Check Network icon (for packets received and sent) / ADSL lights for data in non browsing mode. Check data usage pattern in Mobile. If the outgoing is unusually high, then it is very likely that the system is compromised.
- Type “ ipconfig/displaydns” in command prompt and look out for any URLs which you have not accessed recently.
- Always be cautious while opening attachments even from the known sources. Try to use non native applications for opening attachments. Example for word document use, WordPad to open the attachment.
- When in doubt, better to format the Internet connected computer rather than doing some “patch works”.

USB storage device (Pen Drive / External Harddisk etc.)

- Damaged / faulty RISM should never be handed over to outsiders / manufacturer for repair.
- Sensitive information should be stored on removable media only when required in the cases of assigned duties.
- All media must be stored in a safe, secure environment
- All media must be handled with care and it must be ensured that it is not kept near magnetic material and not exposed to extreme heat or pollution;
- The computers should be enabled with “Show hidden file and folders” option and “Hide protected operating system files” should be disabled to view hidden malicious files in USB storage devices.
- Make sure there is no hidden file and folders present in the Media.
- Autorun/Autoplay feature should be disabled in all the computers.
- Avoid Baiting. (Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer). Do not use any electronic storage device unless you know its origin is legitimate and safe.
- Scan all electronic media for Malware before use.

Smart device – Best practice

Smart device is a device having any of the features like computation power, Internet access, storage capability, camera, recordings, GPS, etc. Smart phone, Tablets, etc. falls under this category.

Most of the Smart Phones and Tablets (Tabs) are having equal computing power of a normal Desktop / Laptop systems. These gadgets are capable of delivering many services on Video, Voice, GPS and other computational apps like any other computer. Therefore, all cyber security issues related to computers are also applicable to these devices. Following are some of the security concerns of Smart devices:

- These are equally vulnerable to malware attacks and data leakages as ordinary Internet connected computers.
- More application, features and service are available on Smart device for exploits than ordinary feature phones.
- These gadgets are known to be used for bugging (audio and video), monitoring call details, contents, SMS monitoring, sending malicious SMS, Emails, spoofing, and other malicious activities without the knowledge of the user.
- Android and IOS platform based Smart Phones and Tabs are known to have multiple vulnerabilities, which are being widely exploited by the attackers and adversaries.
- Smart device must not be used for sensitive telephonic conversation. The Wi-Fi and blue-tooth should be kept in turned-off mode.
- A low-end basic mobile phone without camera / internet / Wi-Fi may be carried for sensitive voice conversation and contact details.
- Internet connection in the Smart device will normally be kept in off-mode and it will be made on on need basis to access internet.
- No free Apps should be loaded in the Smart device.
- During repairs, do not leave Smart device unattended to deny the possibility of installation of malware.
- Relevant anti-virus software should be installed in the smart device.

- If the Smart device gets de-activated for any reason for few hours / one day, the service provider should be contacted immediately to ascertain the reason for deactivation.
- If the battery gets unusually discharged very fast or device gets heated up without any user activity, then it is very likely some malicious traffic is consuming battery.
- Free Wi-Fi should not be used at public places such as Airport. Turn off blue-tooth and Wi-Fi when use of the same is not required for operational purposes. Even when the same is in use, set default blue-tooth / Wi-Fi configuration to "non-discoverable".
- Compromised smart device should not be connected with computer even for the purpose of charging.
- Turn off the applications which are not needed.
- When device is idle, it should get locked and require a password / pin or swipe pattern. Set the device to lock in relatively short time.
- Don’t reply or click on link on SMS or messages sent by strangers.
- Don’t jail-break your device as jail-breaking removes the restrictions on which apps can be installed or not installed. This removes the protection set by the company.
- Watch for unauthorised GPRS/data connection during idle mode of the Smart device.
- Check the memory frequently if any unusual data is stored there. Malware stores temporarily, the data collected in the memory of the phone till the same is sent to the destination.
- Suitable non-transparent tape/sticker may be applied to block the camera view.
- Think before you click, download, forward, or open. Before responding, registering, downloading or providing information, get the facts. No matter how tempting the text, image, or application is, if the download isnt from a legitimate app store or the site of a trusted company, doesnt engage with the message.
- Understand the terms of use. Some applications claim extensive rights to accessing and leveraging your personal information. If the app requires more access to your account and/or device than is needed to run the

service, do not continue. In addition, be aware that terms can change over time. Review your terms of use often.

- Be cautious with public Wi-Fi. Many Smartphone users use free Wi-Fi hotspots to access data (and keep their phone plan costs down). There are numerous threats associated with Wi-Fi hotspots. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.
- Disable Bluetooth and Near Field Communication (NFC) capabilities when not in use. Capabilities such as Bluetooth and NFC can provide ease and convenience in using your Smartphone. They can also provide an easy way for a nearby, unauthorized user to gain access to your data. Turn these features off when they are not required.
- Enable encryption. Enabling encryption on your Smartphone is one of the best ways to safeguard information stored on the device, thwarting unauthorized access.
- Securely dispose of your device. With the constant changes and upgrades in the Smartphone market, many are upgrading their devices on a regular basis. It is important that you wipe the information from your Smartphone before disposal. Additionally, make sure any SD cards are removed and erased. If you are not redeploying the SIM card to another device, then make sure your personal information stored on the SIM card is erased or destroyed.

Social Networking – Best practices

- Do not store any information you want to protect on any device that connects to the Internet.
- Always use high security settings on social networking sites, and be very limited in the personal information you share. Monitor what others are posting about you on their online discussions.
- Use anti-virus and firewall software. Keep them and your browser, and operating systems patched and updated.
- Change your passwords periodically, and do not reuse old passwords. Do not use the same password for more than one system or service. For example, if someone obtains the password for your email, they can access your online banking information with the same password.
- Do not post anything that might embarrass you later, or that you dont want strangers to know.
- Do not automatically download, or respond to content on a website or in an email. Do not click on links in email messages claiming to be from a social networking site. Instead go to the site directly to retrieve messages.
- Only install applications or software that come from trusted, well-known sites. “Free” software may come with malware. Verify what information applications will be able to access prior to enabling them. Once installed, keep it updated
- Avoid accessing your personal accounts from public computers or through public Wi-Fi spots.
- Disable Global Position System (GPS) encoding. Many digital cameras encode the GPS location of a photo when it is taken. If that photo is uploaded to a site, so are the GPS coordinates, which will let people know that exact location.
- Whenever possible, encrypt communications with websites. It may be a feature (like HTTPS site rather than HTTP site) social network sites allow you to enable.
- Beware of unsolicited contacts from individuals in person, on the telephone, or on the Internet who are seeking corporate or personal data.
- Monitor your bank statements, balances, and credit reports.

- Do not share usernames, passwords, credit cards, bank information, salaries, computer network details, security clearances, home and office physical security and logistics, capabilities and limitations of work systems, or schedules and travel itineraries.
- No legitimate service or network administrator will ask you for your password.
- Do not provide information about yourself that will allow others to answer your security questions—such as when using “I forgot my password” feature.
- Be thoughtful and limit personal information you share such as job titles, locations, hobbies, likes and dislikes, or names and details of family members, friends, and co-workers.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.
- Do not click advertisement shown in the social web pages

Email Communication – Best practices

- Auto save of password should not be enabled.
- Users must check their last login details while accessing the Email account.
- Use of encryption and digital signature certificate (DSC) may be considered for mails deemed necessary.
- Email IDs should have a strong password (at least 13 characters with alpha numeric and special characters)
- Once in every 30 days the email passwords should be changed.
- Logout properly from mail accounts.
- Before opening any attachment, the same should be scanned through an updated anti-virus for malicious contents.
- Do not keep mails in Inbox, sent box, draft, etc. which are no longer required.
- User should type the complete URL in the browser instead of clinking links from other sources.
- Before accepting the SSL certificate, the user should verify the authenticity of the certificate.
- Make a habit of clearing history from the browser after each logout sessions.
- Do not open / forward / reply to suspicious E Mail. Do not click any URLs mentioned in the body of the E Mail text.
- Be cautious of Tiny URLs in Email contents.
- Do not open attachment having extension :EXE, DLL, VBS, U64, SHS, PIF , SCR Typical example .txt.exe , .doc.exe
- Some malicious program starts executing as soon as they appear on the Outlook Express preview pane. Disable that option (view -> layout -> uncheck “show preview pane”). Do not open unsolicited or unexpected attachments. If you can not verify an attachment is legitimate, delete it.
- Do not log in to web sites or online applications unless the login page is secure (HTTPS). Do not enter personal or sensitive information online unless you are using a trusted, secure web page.

Wi-Fi Device – Best practices

- Information/Data on the Wi-Fi Network should always be in the encrypted form.
- Do not connect the access point directly to the wired network. As there is a chance of compromised wireless client in turn effecting the systems in the wired network, a firewall and an antivirus gateway should be placed between the access point and the wired network
- In order to allow authorized users to connect to the access point, wireless clients should be provided access based on MAC address.
- Do not auto-Connect to open Wi-Fi Networks.
- Do not use WEP encryption use WPA2 or higher graded encryption
- Change your SSID (Wireless Network Name)
- Turn off SSID broadcasting.
- Change the default passwords while configuring the access point.
- When the number of users accessing the access point is less, it is recommended to disable the DHCP service. As this may make the attackers easy, to connect to the network once they get associated with the access point.
- Update the firmware of access point. It will reduce the number of security loop holes in the access point.

Password – Best Practices

- Passwords must be changed at regular intervals.
- Always use different passwords for different accounts.
- Do not share passwords with anyone.
- All passwords are to be treated as sensitive.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not reveal a password on questionnaires or security forms
- Always decline the use of the "Remember Password" feature of applications
- All users should be aware of how to select strong passwords.
- Strong passwords contain combination of lower case characters, upper case characters, numbers, “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";<>/ etc).
- Contain at least thirteen alphanumeric characters (except in the case of BIOS, if the same is not possible).
- Weak passwords have the following characteristics:
    - The password contains less than thirteen characters
    - The password is a word found in a dictionary (English or foreign)
    - The password is a common usage word such as: Names of family, pets, friends, colleagues, Movie / Novel / Comics characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaaaa, qwerty, asdfg, zxcvb, etc.
- Password history should be enforced wherever possible to ensure that the users are forced to select different passwords with a user account.
- Maximum password age should be configured to enforce the period of time (90 days) that a password can be used before the system forces the user to change it.
- Always use different passwords for different accounts.
- Do not reveal a password in email, chat, or other electronic communication.

- Do not speak about a password in front of others.
- Do not hint at the format of a password
- Do not reveal a password on questionnaires or security forms

Social Engineering – best practices

Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email.

- Some emails entice the recipient into opening an attachment that activates a virus or malicious program in to your computer.
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a persons authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Dont send sensitive information over the Internet before checking a websites security. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
- Take advantage of any anti-phishing features offered by your email client and web browser.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.

- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Dont make you mobile phone as a source for your personal data, which is dangerous if it falls in to the hands of strangers. It is advisable not to store important information like credit card and bank cards passwords, etc in a mobile phone.
- Note the IMEI code of your cell phone and keep it in a safe place. This helps the owner to prevent access to the stolen mobile. The operator can block a phone using the IMEI code.