Information Security Manual

For safe usage of IT

(For General Users)

Published by -

Information Security Dept.

Corporate Centre,

CBD Belapur, N. Mumbai
Dear Colleague,

**Information Security Basics for Safe Usage of IT**  
(For General Users)

Information Technology has become integral part of the Operations in the Bank and as such use of IT for bringing in operational efficiency is bound to increase. All employees are end users of IT.

Reserve Bank of India in its circular issued in April’2011 has categorically defined the Roles and Responsibilities of end user. The responsibilities include –

- Maintaining confidentiality of log-in password(s)
- Ensuring security of information entrusted to their care
- Using bank business assets and information resources for management approved purposes only
- Adhering to all information security policies, procedures, standards and guidelines
- Promptly reporting security incidents to management.

Bank also has regulatory obligation to provide adequate capital towards Operational Risk. IT Risk is one form of Operational Risk associated with the use of IT in the Bank. IT related events like fraud, downtime, hacking, data leakage etc. can potentially impact the business.

We being the end users of the IT should be aware how to safeguard ourselves and in turn the Bank from untoward IT related incidents.

Therefore to bring basic awareness about information security in day to day usage of IT, our Information Security Department (ISD), Corporate Centre has brought out handy booklet on IS prescriptions.

I hope you will find the document simple to understand. I expect that all employees of the Bank follow the prescriptions therein, in day to day operations, which should bring down IT risk in the Bank.

Dy. Managing Director  
& Chief Risk Officer

Date: 01.07.2015

Visit ISD website at State Bank Times > Departments 1 > Information Security
The IS Policy version 4.0 has Thirteen Policy Categories and related Procedures & Guidelines, as below –

<table>
<thead>
<tr>
<th>Policy Category No.</th>
<th>Policy Category Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Human Resource Security ***</td>
</tr>
<tr>
<td>2</td>
<td>Asset Management</td>
</tr>
<tr>
<td>3</td>
<td>Access Control</td>
</tr>
<tr>
<td>4</td>
<td>Cryptography</td>
</tr>
<tr>
<td>5</td>
<td>Physical and Environmental Security</td>
</tr>
<tr>
<td>6</td>
<td>Operations Security</td>
</tr>
<tr>
<td>7</td>
<td>Communication Security</td>
</tr>
<tr>
<td>8</td>
<td>Mobile Device</td>
</tr>
<tr>
<td>9</td>
<td>Information Systems Acquisition, Development and Maintenance</td>
</tr>
<tr>
<td>10</td>
<td>Supplier Management</td>
</tr>
<tr>
<td>11</td>
<td>Information Security Incident Management</td>
</tr>
<tr>
<td>12</td>
<td>Information Security Aspects of Business Continuity Management</td>
</tr>
<tr>
<td>13</td>
<td>Compliance</td>
</tr>
</tbody>
</table>

*** Policy Section 1.3 “Acceptable Usage Policy” & Policy Section 1.4 “Social Media Usage Policy” are most important for End Users and mandate to follow security standards on below areas –

<table>
<thead>
<tr>
<th>Section / Sub-Section No.</th>
<th>Name of Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.1</td>
<td>Desktop and Laptops Usage</td>
</tr>
<tr>
<td>1.3.2</td>
<td>Mobile and Portable Devices</td>
</tr>
<tr>
<td>1.3.3</td>
<td>Password security</td>
</tr>
<tr>
<td>1.3.4</td>
<td>Email Usage</td>
</tr>
<tr>
<td>1.3.5</td>
<td>Internet Usage</td>
</tr>
<tr>
<td>1.3.6</td>
<td>Document and Storage Security</td>
</tr>
<tr>
<td>1.4</td>
<td>Social Media Policy</td>
</tr>
</tbody>
</table>
1. Information Security is all about ensuring –

**Confidentiality**

**Integrity &**

**Availability**

of Data & Services

Compromise of any or all of the above would have negative impact on Confidence, Interest and trust of our Customers, Share Holders, and Regulators (like RBI) in the Bank.

- “Confidentiality” means information is accessible only to those authorized to have access.
- “Integrity” means safeguarding the accuracy and completeness of information and processing methods
- “Availability” means ensuring that authorized users have access to information and associated assets as per commitment when required

Any laxity in ensuring CIA would result into negative feedback, negative publicity in media, by word of mouth, litigation, penalty, dent in Brand Equity etc.

Maintaining CIA in the true spirit is our collective responsibility. Technological or Operational frauds committed would find users’ compromising one / many of CIA – by at of commission or omission.

Bank also has internal mechanism to monitor, correlate, analyze and investigate the users’ activities to catch hold the culprits and take punitive action, as the case may be.
2. Information Security in the Bank –

The Bank has put in place Robust and Agile Information Security (IS) framework in line with the Business strategy and emerging Risks.

a. Information Security Dept (ISD) –

- The Information Security Dept. headed by General Manager and Group Chief Information Security Officer (GM & Group CISO) reports to the Head of the Risk (i.e. DMD & CRO) through CGM (Risk Management) and not to the Head of the IT.
- The GM & Group CISO also reports to the Information Security Committee of the Bank, which is headed by Managing Director & Group Executive (National Banking).

b. IS Policy and related Procedures & Guidelines –

- The “IS Policy, IT Policy and related Procedures and Guidelines” is approved by the Board. The same is reviewed periodically.

c. Technology –

- The layered security technologies are deployed to secure Bank’s setup from attacks from Perimeter and from within the Bank.
- Technology enabled the Bank to provide access to users on “Need to Know” and “Need to Have” basis.
- Various Security Tools / Technologies like Firewalls, Intrusion Detection / Prevention Systems, Web Application Firewalls, Anti-virus, Active Directory Setup, Biometric Authentication System, Internet Proxy Gateway, Patch Management system, Privileged Identity Management, Anti-Phishing etc. have been deployed.
d. State Bank Security Operations Centre (SBSOC) -

- The SBSOC has been setup for Real-time Monitoring, Analysis, Correlation and Incident Management based on the logs generated by IT Assets.

- The SBSOC has capabilities to **monitor users’ activities like Internet usage** (how much time spent on internet, which websites visited etc.), **virus infection** on PCs / Servers, **which programs installed on desktops / servers**, **wrong login attempts** (password guessing) and other unauthorized activities. The SBSOC thus has forensic capabilities.

e. Global Accreditations –

- Bank has achieved various Global Accreditation like ISO 27001 for Information Security Management Systems (ISMS), ISO 22301 for our Business Continuity Management System (BCMS), Payment Card Industry Data Security Standards (PCI DSS) and SSAE 16 for critical applications / IT Setup & related operations

f. IS Awareness –

- IS Awareness among operating staff, system administrators, vendors is key to securely maintain the systems and run operations.

- Bank has been running ongoing security programs for awareness of its own workforce through sessions, quizzes, eLearning lessons etc

- The screen savers running on your office desktop are basic but important security tips in day to day usage of IT.

- Bank has been observing Computer Security Day in which Honourable Chairman addresses Bank’s entire workforce through Video Conferencing and to customers through media channels.

- IS Awareness is spread among customers by publishing advertisements in news papers. We recommend Branches and Offices to spread IS Awareness among customers on safety measures to be taken by them while using ATM, INB, Mobile Banking like maintaining confidentiality of their credentials etc.
3. Acceptable Usage Policy & Social Media Usage Policy

As mentioned above, general users of information systems must adhere to digital hygiene / standards to safeguard Own and Bank’s interest.

a. Desktop and Laptops Usage

Office desktops / PCs contain critical and confidential data and files. Depending on the role, it could contain customer information like their contacts, loan / deposit account details, inspection reports, office Notes, Policies, Circulars, Board / Committee Notes, Disciplinary Actions etc.

Therefore, it would be myth if one wrongly assumes –

- There is nothing important on my computer.
- As Anti-virus is installed and desktop is in Active Directory and therefore it is fully secured, so I don’t have anything to contribute in the security of my computer.

Every new Desktop / PC / Windows Server deployed in the Bank must be brought under Active Directory and Anti-virus be installed immediately.

For security of your desktop, following minimum basic but important practices should be followed –

- Always lock your desktop while leaving seat, even for a minute or so by pressing Windows key and L key simultaneously. Anyone can unauthorizedely access and exploit your system if it is not in locked state.
- Do not create or copy documents or create shortcuts on the home screen of desktop. Although it might give comfort, it might also invite risk. Another person with intention to unauthorizedely access your documents will have ease to locate these documents.
▪ Anti-virus is very important for ensuring safety of data/files from virus, worms, Trojans, spyware, key loggers infection.

▪ Anti-virus automatically scans email attachments, documents opened from internet etc., cleans virus/quarantines uncleaned files. Virus not cleaned by the Anti-virus should be reported to user’s manager.
▪ Users should not attempt to uninstall, disable Anti-virus.
▪ Check that the latest version Anti-virus and Virus Pattern are running on your desktop/PC. Steps to verify the same are as below –
  ✓ In the Right corner of Task Bar look for blue circle icon with lines as shown in picture given below. If this icon is present it means that Trend Micro antivirus is present in your system

  ✓ Many times icon may not be displayed in the task bar due to settings made in Windows to display icons. You may then check the same by following steps:
  ✓ Click on Start icon in the left side of the task bar – Select all programs option – search for Trend Micro Office Scan Client option. If the same is present click on it, you will find following options:

  ✓ Right click on Trend Micro antivirus
    Blue icon on the task bar ➔
    Click on Component Version.
✓ The version and release date of the latest file may be verified with the information available on State Bank Times – Antivirus (on the main screen).

- Active Directory disables USB & CD / DVD drive on PCs, Users should also not connect pen drive, dongle, data cards, cable internet, modem etc. to PC. Use of CD-ROM, DVD is prohibited.
- Users should not access or download personal music, video files etc.
- Users should get their desktops formatted/repaired by designated AMC service providers under supervision of State Bank personnel. Users should not attempt to fix the hardware or software related problems on their own. It might make warranty / guarantee VOID.
Successful backup of critical applications or data should be ensured daily / periodically and before formatting of desktops/laptops so that same can be restored back.

- Users should not install any software, freeware, shareware or application on their desktop/laptop that is not authorized for State Bank’s business.

- Users on whose PC / Server such software runs shall be solely responsible for Copyrights / IPR violation, Legal and Penal actions as per IT Act etc.

b. Mobile and Portable Devices

Mobile and portable devices are laptops, tablets, mobile phones (smart phones). Mobile Phone / Tablet has become one stop gadget and is used as digital diary, phone book, Still & Video camera, Audio Recorder, photo / video album, Walkman / Radio, PC (for accessing email, processing documents like Word/Excel/PowerPoint etc), clock / alarm, Wi-Fi hotspot, gaming console, news papers & magazines, international and inland letter / postcard, Banking platform and will not be exaggeration if we say it is incidentally used for making calls.

With so many activities being done by a mobile device, security of mobile and portable devices is all the more necessary, because of following reasons –

- These are used on the move – like when travelling, in public places, home, office etc. and also prone to misplaced / loss.
- These devices are not connected to the Bank’s safeguarding systems like Active Directory, Anti-virus setup, Internet Proxy and therefore users are not restricted from installing applications of their like, visiting any websites, downloading / installing any kind of contents from websites and social networking sites / applications like Facebook, Whatsapp etc.
- The vulnerabilities in the operating systems (say Android, iOS etc) and installed applications might compromise the security of these devices.
- Installed applications like Truecaller, Whatsapp, Facebook etc. might be exploited to compromise confidentiality of the data by extracting contact details and storing the same on their cloud system / sharing with others / marketers etc.
- New age malwares (malicious software) installed on user’s mobile phone / tablets can allow attacker to impersonate the user for making calls / send SMS, receive SMS etc.
- Take adequate measures for physical protection of devices like not leaving device unattended in public places or while travelling.
- Loss of portable device should be reported immediately to the local police and to the appropriate authority.

- Portable device users should be responsible for the security of their device and the information it contains.
- Users should not connect their personal laptops or mobile devices to State Bank's Network.

- Personnel, to whom State bank owned laptops or any other Portable devices are issued, are responsible for its safe custody.
- Employees shall not loan their laptop or allow it to be used by others such as family and friends.
- Laptops, if required to be left in the office at the end of the workday, shall be locked in a secure manner.
- All mobile computing devices should be tagged with the contact details of the associated user. Where possible the asset tagging should not identify the device
as belonging to State Bank. Such identifications may make the device a more attractive target for theft.

c. Password security

- Users are responsible for all activities originating from their User credentials.

  - Password should be treated like signature; if it is not complex, sufficiently long and secret, it could be a target of successful guessing and misuse by fraudsters.
  - Password should be easy to remember but difficult to guess.

- Own name, short form of own name, own initials, names of family, friends, co-workers, company or popular characters, own date of birth / telephone number / own vehicle number are easily guessable by others and therefore should be avoided in password.

- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc or combination with numbers like secret1, 1secret etc. should not be used in password.

- Dictionary words like umbrella, sunshine, kite, monkey, prince, money or phrases like iloveyou, iamaboy, letmein should not be used.

- Websites use CAPTCHA to avoid password guessing by automated tools – called “Dictionary Attack”. CAPTCHA
Don’t share passwords with anyone including colleagues and IT staff or should not ask others (including customers and colleagues) for their passwords.

Password should be changed at least once in 90 days or when you suspect it has been compromised.

If your account is locked out before 3 invalid attempts, it could be because someone else was trying to guess the password. Report it to your manager. Change password immediately.

Don’t write your password, instead memorise it.

Passwords of Root / Administrator / Admin / Super user of critical systems like OS of Servers, Oracle, Routers, Business Critical Applications etc. can be jointly held and securely kept in sealed envelope.

Systems with no password are major risk.

**Strong Password**

Strong password has following features –

- minimum length of 8 characters
- at least one numerical (0,1,2,3 .... 9)
- at least one special character (! @, #, $,%,^,&,*,(,))
- Mix of Uppercase and Lowercase alphabets (A, B, C, a, b, c etc.)
- Browser’s facility “Remember my credentials” / “Remember Password” should not be used. Because, although the browser might not be storing your password, but a token that represents you is a token, called “cookie” that represents you gets assigned. If this cookie is stolen, a malicious user could use that to log in as you without knowing your password.

- Uncheck / keep blank the setting “Offer to save you web password” in Chrome’s setting.

- To disable remember password, in Internet Explorer, you can go to “Tools - > Internet Options - > Contents-> AutoComplete Setting”. Uncheck “Forms” and “User names and passwords on forms”.

- There would be similar settings in other browsers which can be used to disable the feature of remember password.

- Various websites also offer to remember password. It is recommended to not opt for it.
d. Email Usage

- State Bank's electronic mail system (Enterprise Messaging System – EMS) should be used for Bank’s business communication.
- Use of Bank’s official mail account for personal purposes is discouraged.
- Due to its ease of use, faster and efficient communication and to save papers, marking copy to multiple stakeholders, Bank’s EMS has gained popularity during the last few years. As such emails are used for –
  - day to day communications
  - intra-office (within branch / office / dept) and inter-office communications
  - communication to and from customers
  - important instructions / communications from administrative offices

- Users owning the email account are fully responsible for the content of email originated, replied or forwarded from their account to other users within or outside the Bank.

  - Email sent from Bank provided email ID is as good as letter on Bank’s letter head.
  - Bank may intercept or disclose or assist in intercepting or disclosing Email communications to ensure that email usage is as per Bank’s IS Policy. User communications should not be considered private as also not send inappropriate contents.

- Inappropriate contents include contents that –
  - Are libellous, defamatory, offensive, racist, Anti-National messages, obscene remarks or for private business activities, personal gain or profit or job search
  - May damage the reputation of the Bank, contain viruses, worms or malware
  - Chain mails containing virus hoaxes or for charitable fund raising campaigns, political advocacy efforts, religious efforts, or personal amusement and entertainment and others.
  - Unsolicited emails to large number of users which can be considered as mail spamming.
  - Using email system to copy and/or transmit any document, software or other information protected by copyright or any other law.
- Mails to external entities containing instructions or contents that require authorization of a superior in the normal course of Banking, unless such prior authorization is obtained.

- Confidential or secret information should be encrypted or password protected when transmitted over email. It is recommended to start subject line with “Confidential”, “Secret”, “Private & Confidential”, “Internal” and then mention subject. It then becomes responsibility of recipients to ensure confidentiality / privacy of the matter reported.

- Please note that digitally signed doesn’t means that scanned copy of signature is pasted in the mail body.

- Digital Signature is a mechanism by which the sender encrypts the message by using “Public” key of intended recipient. The recipient applies own “Private” key to decrypt the message.

- In this process “Non Repudiation” is ensured.

- It is difficult to legally establish the identity of sender of email messages unless they are digitally signed. Emails that are not digitally signed should not be used for critical transactions requiring legal authentication of sender; like execution of contract, payment or transfer of money, issuing official notices to external world. Emails that are not digitally signed should not be used for critical transactions requiring legal authentication of sender.

-Instances have been noticed that Branches have acted on the basis of emails to transfer funds from one account to third party accounts. The customer
whose account was debited in the process denied having sent such email. Email ID can be spoofed for sending fraudulent emails.

- As per extant instructions, the transactions between the accounts under the same CIF, the same branch and same capacity are allowed over email.

Don’t provide Bank’s email account to any mailing lists / internet websites / Internet newsgroup / discussion board. These websites, persons might provide your email ID to their interested parties and likewise the email ID would get circulated to number of unknown people / entities.

Providing email ID like above might result into receiving emails like marketing, lottery, draws, phishing etc. called SPAM unnecessarily flooding inbox with no space left for official emails.

- Do not open / download attachments from emails howsoever appealing they are, if email is from unknown sender or even the attachment is not expected from known person / official.

- These attachments might drop virus, worms, Trojans, Botnets into the system and transmit data / information in bits and pieces to the hacker.

- The contents like photo, video etc. in email attachments might also contain hidden messages behind them which cannot be seen in normal course. This technique is called Steganography technique (used by terrorist, defence, secret services). The user responsible for creating / forwarding such emails could be held responsible.

- Trojans like Advance Persistent Threat – APT attack have resulted into financial and IPR losses to companies, embarrassment and action on officials responsible for the compromise.
- The malware infection can also make the system Zombie (of which owner is unaware) and forward transmissions (including spam or viruses) or launching DDoS attack on other computers on the Internet. Such system is controlled by Master (called BotNet Command & Control – C&C) system unknown to user.

### Botnet Operation

- Users should not access State Bank's email account from insecure internet connection like open Wi-Fi, public hotspots, insecure cybercafé etc.
- Users should promptly report all suspected security vulnerabilities that they notice with the Email account to authorized personnel.
- Archive emails file stored locally on the user’s machine should be protected by password. In the Microsoft Outlook it can be done by following the options in the menu “Tools->Options->Mail Setup Tab->Data Files Tab”. Select the file to be protected by password and click on “Settings” button. Click on “Change Password”. Change the password.
In case you are adding a new data file, the system will automatically ask you the password.

How to identify SPAM email?

When the email id, contact information is given on various websites, surveys, conferences, hotels, magazines etc. they might share the same with their partners, their sister concerns and likewise the chain gets extended without any limit. These email IDs and contact information might land in unscrupulous elements (domestic and foreign) and thus get added in emailing / SMS list. Thus people whose contact information gets into their hand, would start receiving various offers via emails / SMS and even social engineering emails like Phishing etc.

SPAM emails are unsolicited bulk email and sent to numerous recipients informing potential victim about having won lottery, receipt of Goods, recruitment, custom clearance, business partnership, update Bank account information due to security reasons etc.
Typically, spam email would have no email ID in “To” or “CC”

As the spam is sent to billions of recipients, it would not be addressed specifically to recipient / victim. Instead of Dear Sh. Makarand, it would address recipient as “Dear SBI Customer”, “Dear Valued Customer” etc.

It would encourage the recipient to click on a Link or open an attachment which could lead victim to Phishing Site or download virus, Trojan etc.

Types of Email IDs and their purpose

- There are different types of email addresses in the EMS –
  - Email address provided to individual official like makarand.kedare@sbi.co.in
  - Designation / Role based email address like gm.ciso@sbi.co.in
    - Wherever possible, designation based email addresses may be created.
    - It implicitly conveys authority of email ID holder.
    - In case of individual email ID case, when the person gets transferred / ceased to be in service, the sender of email wouldn’t know and would
keep sending emails to him/her. This risk is not there in designation / role based email addresses, as new incumbent would own the email ID.

✓ New incumbent (email id owner) should immediately change password of such email id after assuming charge of seat / office.

e. Internet Usage

- Authorised Users should access Bank’s Internet for business purposes and restrict non-business activities over Internet.
- Bank has Corporate Internet Proxy setup. This setup is protected by firewall which prevents any connection from outside the Bank to inside system. This setup also secures our systems from viruses and malicious contents from entering into our systems.

- Users should access Internet only through Bank’s Corporate Internet Proxy setup and not by using Data Card, Modem, Cable Internet on office PC / system.
- Users should use internet facilities in appropriate manner; access to any website that contains potentially offensive material is prohibited and will be held responsible for any misuse of Internet access originating from their account.

- Centralized Internet Access also regulates the websites allowed to be visited by users on the basis of their role and requirement. Websites like RBI, SEBI, IRCTC, Government departments, authorities, universities etc. are allowed for all kind of users. If any website is required to be accessed for Bank’s business purpose, the same can be got added by placing a request to Bank’s IT-Networking Dept at GITC, CBD Belapur, Navi Mumbai.
- Users shall be responsible for protecting their Internet account and password.
- Users shall not configure browser to remember web application passwords.
- State Bank reserves the right to monitor and review Internet usage of users to ensure compliance to this policy.
- Users should not use Internet facilities to -
  - Download or distribute malicious software or tools or to deliberately propagate any virus.
  - Violate any copyright or license agreement by downloading or distributing protected material.
  - Upload files, software or data belonging to Bank to any Internet site without authorization of the owner of the file/software/data.
  - Share any confidential or sensitive information of the Bank with any Internet site unless authorized by superior/controller.
  - Post views or opinion on behalf of the Bank unless authorized by top management.
  - Post remarks that are defamatory, obscene or not in line with Bank’s policy on the subject.

Conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting the Bank. In case such misuse of the Internet access is detected, Bank can terminate the user Internet account and take other disciplinary action.

- Users should ensure that they do not access websites by clicking on links provide in emails or in other websites. When accessing a website where sensitive information is being accessed or financial transactions are done, it is advisable to access the website by typing the URL address manually rather than clicking on a link.(Explained in Email Security above and below in Phishing section)
f. **Document and Storage Security**

- All documents containing confidential or secret information should be marked as “confidential” or "secret" both in electronic and print format. Care should be taken to ensure confidentiality while these documents are transmitted over email, fax or other communication media or during printing and photocopying of documents.

![CONFIDENTIAL]

- All removable media should be labelled as “confidential” or "secret" (as applicable) if it is used to store “confidential” or "secret" documents.

- Users should adopt a clean desk policy for papers, disks and other documentation.

- Obsolete documents/papers should be destroyed/shredded using secure measures. Expired and bad storage media should be destroyed before disposal.

![BAD HABBIT]

![Paper Shredder]
- Warning notices should be displayed on the fax coversheets to the effect that the message is meant for the addressee only and the use of the message by any other party may be unlawful.
- Confidential and secret documents should be stored in locked fire-proof cabinets.
- Users should keep a backup copy of important documents in a secure manner. The backup can be taken by keeping a copy of the documents on removable media.

Secret or confidential information should not be discussed in the presence of external personnel or other Bank employees who do not ‘need to know’ that information.

- Users who have been authorized to use the Smart Cards or Private Keys should safeguard them.
- No User should transfer customer information classified as confidential such as (Name, account details, balance etc.) to any person/place internal or external to State Bank.
- No confidential information and mails related to staff/ Suppliers/ customer /State Bank should be put on office notice boards or posted onto Internet.
- Information classified as confidential shall only be accessed when authorized by Competent Authority as also be disclosed to named individuals. Proper measures should be taken avoid unauthorized or accidental disclosure.
- Confidential or secret information should be disclosed to other State Bank Group Company only after the written permission of the Competent Authority owning the information.
- Secret or confidential information could get revealed unintentionally due to unsafe practices. Care should be exercised in the following scenarios to protect sensitive information -
  ✓ Reading confidential documents in public places
  ✓ Discussing confidential information in public places
  ✓ Working on laptops in public places
✓ Answering to queries over phone to unverified persons
✓ Providing information to suppliers
✓ Chatting over social media

g. Social Media Policy

- Social media has made inroad into our daily routine life. Facebook, LinkedIn, WhatsApp, Instagram, Twitter, YouTube, Blogs, Chats, Discussion Forums, Gmail, Yahoo mails etc. are used to communicate with masses / groups like friends, relatives, colleagues in one go.
- Employees should adhere to all of State Bank's policies/instructions at all times, whether blogging and social networking for business or personal reasons, via State Bank's computer system and accounts or user's own private accounts and personal devices.
- Even in case of personal profiles on Facebook, Twitter, LinkedIn, YouTube etc., if privacy filters are not set properly, the contents can be seen, downloaded, and shared by public in general.
- Bank has social media presence in the form of its own Corporate Website, has presence on Facebook, Twitter and YouTube.
- Bank also has in-house Social Media facility called “SBI Aspirations” which can be used for sharing Views, Ideas, Discussion Forums, Chats, Blogs and much more. Our Top Executes extensively use this media for communicating and connecting with employees. Most of the features as available in Facebook, LinkedIn are also available in SBI Aspirations.

Bank’s Presence in Social Media / Internet

- Corporate Website - https://www.sbi.co.in/ and also has presence in Social Media domain.
- Facebook – https://www.facebook.com/StateBankOfIndia
- Twitter - https://twitter.com/theofficialsbi (Handle @TheOfficialSBI)
- YouTube - https://www.youtube.com/user/TheOfficialSBI
- SBI Aspirations - https://aspirations.sbi.co.in or https://social.sbi.co.in (available on Intranet & Internet)
The contents, views, blogs, photos, videos, audios, response to customers’ queries etc. on the above websites are provided / managed / uploaded by the Bank’s Officials Authorized for the activity.

Employees should ensure the following in Internet sites or Social Media or Social Networking Sites –

- Not to directly or indirectly disclose / refer State Bank’s Name, Logo, URL, Email Address, Contacts, Own Official Capacity.
- Not to directly or indirectly disclose / refer / criticise Bank or Bank’s Officials or Customers.
- Not to Disclose / Refer Bank’s Circulars, Business information, Official Papers, Contents of Bank’s internal or internet facing websites.
- Not to post/express their views / opinion in the official capacity of the Bank.
- Not to engage in collusive behaviour with State Bank’s competitors or employees.
- Not to canvass for any donation, lottery or supplier marketing/business promotional activities/affairs.
- If under the circumstances, employee’s connection to the State Bank is apparent, then users should write in the first person (I, me, my, mine, myself) i.e. on writing on own behalf not speaking / writing as an authorized Bank’s spokesperson.

It was observed that Bank’s officials shared confidential information like circulars, business decisions, meeting agenda, scanned copies, recorded messages etc. through WhatsApp, published on internet based websites, posted on Facebook, Twitter and groups. This is fraught with the Risk and against Bank’s confidentiality norms.

Users might get addictive to Social Networking Sites and Apps and thus valuable time would be lost on these sites. Further, during the course, users might unwittingly / inadvertently share personal and official confidential information. Such users might also become victim of Social Engineering attacks.
Further, if the credentials of Social Networking Channels (Gmail, Yahoomail, Facebook, tweeter etc.) get hacked, the hackers / culprits might blackmail for money and other benefits. They might threaten to post bad contents, photos, tweets, use abusive language or send abusive emails etc. using such compromised credentials. This is also called cyber stalking, bullying.

Various websites like Google provide free storage space on their Cloud. Cloud has security concerns like privacy and integrity. Uploading private contents, photos, documents on such free storage on the cloud is also fraught with risk.

Less you divulge and more you are secured in virtual world of Social Networking Sites and Channel.

h. Security Violation and Incident Reporting

- All users have the responsibility to report suspected information security violations, incidents, and vulnerabilities as soon as possible to the appropriate authority as per Incident Management policy and Whistle Blower Policy.
- Users should report the incidents to their respective manager. User's manager should do a preliminary analysis of the incident, ensure that all details/evidences relevant to the incident are captured as per digital evidence policy and decide the criticality of the incident.
- All information security incidents should be reported by user's manager preferably branch/unit head to IT-RMD through service desk only in the category of "Information Security Incidents".
- Incident should be reported to the required regulatory and government authorities i.e. cyber police, as applicable, by the user's manager preferably the unit head.
- Incidents could result in un-authorized access, disclosure of information, corruption of information or denial of service.
- Users should follow these indicative guidelines in identifying an incident. This list is not exhaustive.
✓ Abnormal system resource usage: If the CPU, memory utilization on a system is very high, the system could have been compromised. Attackers use compromised systems for spreading viruses or attacking other machines leading to high resource utilization.

✓ Users experience slow response: End users could experience slow response times if the application servers or the network has been compromised and is being used for malicious purposes. Virus or worm outbreak could lead to network congestion that would in-turn cause application responses to be slow and unstable. End users should report any drastic drop in application response.

✓ Data corruption: Unauthorized modification or deletion of data or inability to retrieve data in correct format or web site defacement.

✓ Changes in passwords and user-id: Any changes in user passwords, addition/deletion of user accounts could be indications of system compromise. Unauthorized activation of suspended / deleted user accounts

✓ Traffic on non-essential ports: If there is network traffic on ports that are not used by any of the internal applications this could be signs of a backdoor application in the network. The traffic should be tracked and reported by the monitoring team. If the backdoor application tries to traverse the firewall, these would be tracked by the firewall logs.

✓ Existence of unknown user accounts: Normally attackers create new accounts on the systems after they are compromised. Existence of unknown user accounts, especially those with administrative privileges, could indicate that system has been attacked.

- Employees should not report incidents to external entities unless required by legal and regulatory requirements. Employees should seek appropriate authorization before such disclosure.
- Security violation may attract disciplinary action up to termination from the Bank’s Service.
- In case of reporting security violation or incident, uers should collect evidences that may include information:
From as many IT sources as possible (e.g. active, temporary and deleted files, email or Internet use, memory caches, registers, network logs etc.)

From as many non-IT resources as possible (e.g. CCTV, building access logs, eye witness etc.)

From individuals giving due regard to privacy and human rights

i. Other Important Prescriptions

- All employees and external party users should return all of the state bank's assets in their possession upon termination of their employment, contract or agreement.
- End users provided with Electronic / Digital Certificates should carefully read and comply with prescriptions in “Policy Category 4 – Cryptography” of IS Policy.
- For premises that require access cards for access, it is mandatory for all employees, trainees, and supplier personnel to use one’s own access card issued by State Bank for entering and exiting the facility. Tailgating (entering access controlled doors without swiping one’s card) is strictly forbidden.
- Employees visiting other offices shall carry and display their identity cards.
- Every employee, trainee and supplier personnel, who has been issued an access card by State Bank should immediately report loss or theft of card to the issuing authority.
- Visitors in State bank's premises (other than public areas / reception areas / designated visitor areas) should be escorted at all times by a State Bank's Employee.
- Supplier support personnel should produce a letter on the company letterhead stating that the person is an employee of the company and assigned to work with the Bank. Supplier support person should produce their employee id card or any acceptable identity proof for identification.
- All personnel entering the premises should declare, if they are carrying any IT equipment like mobile, pen drives/hard disk or any portable storage media, or laptop. If anything needs to be taken out that should be informed in advance to the guards by respective authority.
4. Security in INB, ATM, Mobile Banking

a. Internet Banking –

- Internet Banking website should be accessed by typing https://www.onlinesbi.com/ in the Internet Browser. Link on other websites or in email should not be clicked to visit INB website. These links might redirect to fraudulent / lookalike website of Internet Banking called “Phishing” Site.
- Internet Banking is secured by SSL (Secured Socket Layer). The users should check that –
  - The website address starts with HTTPS. The “S” in HTTPS stands for Secured.
  - Either the Padlock symbol appears at the bottom of the internet browser or the Address Bar and the Address Bar also turns Green.

- Internet Banking has Login and Profile passwords. Profile password is required by the INB for addition of third party for fund transfer, beneficiary addition and biller addition require additional password in retail application.
- Internet Banking users should be encouraged to register Mobile Number for receiving One Time Password (OTP). Internet Banking user should enter the OTP sent by the Bank for authorising the addition of beneficiary, transaction etc.
- New third party is activated only up to 8:00 p.m.
- There is a cap on funds that can be transferred during the initial five days of addition of third party.
- Bank sends SMS after every transaction, when Profile section is accessed, third party / beneficiary is added etc. Keep track of activities and SMSes received.
When you login, check whether the date and time under “Previous Site Visit” and “Last Login Failed attempt” are as per your last successful login and failed attempt.

- Avoid using Internet Banking in Public Places, Cyber Cafes or if you have suspicion about the system.
- There are malwares like Key loggers, Spywares, Trojans etc. which can reside on the PC / Desktop / system which can capture / record the keys hits on keyboard connected to it.

To avoid key hits being recorded, use the “Virtual Keyboard” on the login screen for entering credential. Virtual Keyboard can be enabled by checking the checkbox

Virtual Keyboard displays the characters at random positions. Whenever the login screen is Refreshed or Virtual Keyboard is enabled, the position of each character would be different than previous instance.

- Change the INB passwords as frequently as possible. Change it immediately on doubt that someone has seen it or seems to be entered / compromised on fraudulent websites etc.
- There are following provisions on the [https://www.onlinesbi.com/](https://www.onlinesbi.com/) for blocking INB login –
  - Either enter correct Login ID and wrong password four times. The Login will be blocked until 12.00 o’clock in the night. Login will get activated after 12.00 O’clock night.
Click on “Lock User Access” link in the login screen. Enter correct details as recorded in the CBS, enter text (called CAPTCHA which is case sensitive) displayed and click on Confirm button. The INB login will be deactivated permanently until you activate it by requesting the branch.

b. ATM –

- ATM Card should be kept securely and should not be given to others.
- ATM PIN should be kept confidential and even should not be written; instead it should be memorised. Keep the card details confidential.
- ATM PIN should not be vehicle number, digits in Date of Birth or easily guessable numbers like 1111, 2222, 1234, 9876, 4567 etc.
- Register your mobile number with the Bank. In case of Card Not Present transactions i.e. for payment using Debit Cards on eCommerce websites, OTP has been made mandatory. OTP is sent on registered mobile number. Transaction alert is also sent on the registered mobile number.
- Customer having Internet Banking can change “ATM Card Limit/Channel/Usage Change”. After logging in click on eServices Menu->ATM Card services-> ATM Card Limit/Channel/Usage Change.
In case debit card is lost, compromised etc., it can be blocked –

- From INB login page
- After login in INB; eServices Menu->ATM Card services->Block ATM Card
- By sending SMS “Block <<last 4 digit of card>>” to 567676

- At Point of Sale (PoS), the debit card should be asked to swipe in your presence and the PIN should be entered by you by hiding keypad.

- Magnetic stripe based cards are vulnerable to Skimming i.e. copying card information. Places like Petrol Pump, Restaurants etc. are vulnerable places where this can happen. Frauds like mobile top up, lucky draw etc. if card is swiped are examples of card skimming.

- Skimming devices can be fitted at the card inserting slot on ATMs, like below. These devices can be used for copying card data from magnetic stripe.
The fraudsters might install a pinhole camera over the keypad to record and transmit/store PIN in sync with the card swiped.

- Fraudsters might also deploy fraudulent keypad to record/transmit PIN entered. The PIN entered in such fraudulent keypad would not be accepted by the ATM (as not being connected to ATM system internally). Thus, after attempting the PIN entry, the customers would get the impression that keypad is not working and would leave the ATM. However, the fraudsters would have obtained the PIN.
- Our Bank’s ATMs ask the customer to enter two digits after inserting the card. If the digits entered appear on the screen, then the keypad is authentic.
- Fraudsters might also stand near you (as if there to help you) and note PIN, they might stand outside ATM and note PIN (called shoulder surfing). If there is a mirror on the ATM, check whether anybody is attempting to see PIN.
- ATMs at crowded places are vulnerable to shoulder surfing.
- Customers should be encouraged to opt EMV Chip Cards which is more secured than magnetic stripe based cards.

![Image of EMV Chip Cards]

c. Mobile Banking –

- Lock your phone with a mPIN or password when not in use.
- Always keep your mobile device in a safe location.
- Download the Mobile Banking application only from the Bank’s site – www.sbi.co.in
- For using Mobile Banking service over WAP, never click on any links. Always type the URL http://mobile.prepaysbi.com/sbiwap/ in your mobile browser
- Check your linked accounts on a regular basis
- Once your transaction is over, logout of WAP mobile banking website and then close the browser
- Delete any SMS from the Bank that might contain your personal information like, user Id, mPIN received at the time of registration, or details sent to you
- Do not part with your ATM card and PIN as this may be misused for Mobile banking registration
d. State Bank Anywhere

State Bank Anywhere a secured and robust mobile application based for Android, Apple and Blackberry mobile phones. The following measures are put in place to protect our esteemed customers.

- No personal information is stored on your mobile phone or SIM card, as INB credentials are used for login.
- The application force closes, if kept idle for 5 minutes.
- The application can only be accessed after proper authentication of customer username and password.
- SSL encryption is used to protect your communication with the Bank.
- Your session ends as soon as you close the application.
- Your session also closes automatically after 5 minutes of idle time.

For further details, visit [https://m.onlinesbi.com/sbijava/mobile/sbf_faq.html](https://m.onlinesbi.com/sbijava/mobile/sbf_faq.html)

State Bank Anywhere (User friendly touch screens)
5. Social Engineering attacks

In this type of attacks, the fraudsters lure / appeal the potential victims to gain confidence to reveal confidential information and use the same for fraud, system access etc. Examples are like –

- “Hello, I am Chairman of Bank calling”
- “Hello, you have won a lottery”
- “I am from Service Desk. Please provide me your password as I need to update your Desktop”
- Click on the link to enter your password.

Phishing

- Phishing is a technique of fraudulently obtaining private information like INB login ID and Password, Debit / Credit Card details, PIN, Date of Birth, Mobile Number etc. Typically, the fraudster sends an e-mail (SPAM as discussed above, which is sent to one and all – not specific to SBI or specific Bank’s customers) that appears to come from say Bank, Credit Card company, RBI, Income Tax etc. requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate like Bank of the victim with company logos and content and has a form requesting personal information.

- Above websites looks like our Bank’s Internet Banking website. However, please note following –
6. Facts

- Nine out of ten employees would unwittingly open or execute a dangerous virus-carrying email attachment
- Two-thirds of security managers felt that the overall level of security awareness is either inadequate or dangerously inadequate
- Nine out of ten employees revealed their password on request

These things don’t happen as a result of malicious intent, but rather a lack of awareness of Security Risks.

7. Top 10 common Security Mistakes

- Passwords on Post-it Notes
- Leaving your computer on, unattended
- Opening e-mail attachments from strangers
- Poor password etiquette
- Laptops on the loose
- Blabber mouths
- Plug and play without protection
- Not reporting security violations
- Always behind the times (the patch procrastinator)
- Not knowing internal threats

The overall key message is that we as an individual employee should have security mindset and be a Responsible User of IT.

--- End ---
KNOW THY ENEMY!

MALWARE CLASSIFICATIONS