IS Compliance to Bank of India Computing Resources

Ref: "Information System Security Policy "

Undertaking

Employee Undertaking

I have read Bank of India's Acceptable Usage Policy document on _____. I recognise and understand that the Bank of India's computing resources including e-mail/Internet systems is to be used for conducting the Bank's business only. I understand that use of this facility for private purpose is strictly prohibited, except when expressly permitted.

I am Aware of my following roles and responsibilities.

Acceptable usage policy covers the following aspects for users:

- Maintaining physical and logical security of user desktops / laptops
- Maintaining antivirus protection on desktops / laptops
- Safe usage of Internet
- Safe email usage and maintaining email etiquettes
- Compliance with license and copyright requirements
- Protecting computer accounts and passwords
- Reporting security incidents and weaknesses
- Not engaging in any activity that leads to security violations

I am aware that the Bank may access and review any materials created, stored, sent or received by me through the Bank network or Internet connection.

I have read the aforementioned document and agree to follow all policies and procedures that are set forth therein. I further agree to abide by the standards set in the document for the duration of my employment / association with the Bank.

I am aware that violations of this ISSP may subject me to disciplinary action, up to and including discharge from employment and any legal action in case of illegal acts that may be initiated by the Bank during my employment / association with the Bank or thereafter.

Furthermore I understand that this policy and document can be amended at any time and I hereby agree to abide by the revised policy and procedures as long as I continue to be the user of the Bank's Information Systems.

_____ _____

Employee Signature Date

_____

Employee Name

Acceptable Usage

IT assets of the bank are provided for business purposes and authorized users should adhere to safe usage practices that do not disrupt business or bring disrepute to the bank. Standards will be defined to include safe usage of desktops, computer accounts, business applications, computer networks and for protection of information in physical or logical form and maintenance of Intellectual Property Rights by the users of information systems.

1 Desktop Usage

1.1 Users are responsible for the security of their desktops and should take adequate measures to restrict physical and logical access to their desktops.

Configuration & Installation

1.2 All desktops will be configured by system administrators as per the secure configuration standards provided by Information Systems Security Formulation and Implementation Team (ISSFIT).

1.3 Users should not install any software or applications on their desktop that is not authorized or not essential to bank's business.

1.4 Users should not connect modems to their machines unless and otherwise approved by the appropriate authority.

Protection Measures

1.5 Necessary measures should be adopted by users to prevent the risk of unauthorized access.

Anti-virus

1.6 Users should not disable the installed anti-virus agent or change its settings defined during installation.

1.7 Users should not disrupt the auto virus scan scheduled on their desktop.

1.8 All files received from external sources should be scanned for virus before opening

1.9 User should report to system administrator on any virus detected in the system and not cleaned by the anti-virus.

Laptop Security

1.10 Laptop users need to adopt the following measures

- Ensure that laptop is configured as per the secure configuration documents provided by ISSFIT.
- Enable boot level password in the laptop.
- Encryption or password protection should be enabled for protection of data.
- Antivirus agent with latest signatures should be installed, before laptop is connected to the LAN.
- All necessary patches / hot fixes for the operating system and applications installed should be periodically updated.
- Log off laptops when not working for extended period and enable screen saver with password for protection during short period of inactivity.
- Backup critical files from laptop to your desktop or removable media like CD/floppies.
- Take adequate measures for physical protection of laptop including not leaving laptops unattended in public places or while traveling.

1.11 If the laptop has modem / dial up facility for Internet, users should disconnect Internet connection before connecting to the bank's LAN.

1.12 Loss of laptop should be reported immediately to the department head and ISSFIT.

1.13 Third party laptop connecting to the bank's network should be restricted. Prior approval from IT head should be taken before connecting third party laptops to bank's network.

2 Password Security

2.1 Users are responsible for all activities originating from their computer accounts.

Password construction

2.2 Users should choose passwords that are easy to remember but difficult to guess.

2.3 The password shall not be based on birthdays, computer terms, known jargons etc.

2.4 The password shall not be a word or number like aaabbb, qwerty, 123321 or any of the above spelled backwords.

2.5 The password shall be a combination of upper & lower case characters (Ex:- a-z, A-Z) digits (Ex:- 0-9) and special characters($,*,# etc.)

2.6 The Password history should be maintained and the last 2 passwords shouldn't be usable.

Password Protection

2.7 Users should not share their passwords with anyone including colleagues and IT staff.

2.8 Users should ensure that nobody is watching when they are entering password into the system.

2.9 User should not keep a written copy (in paper or electronic form) of password in easily locatable places.

2.10 Users should change their password regularly.

2.11 User should report to the system administrator if account is locked out before 3 bad attempts.

3 Internet Usage

3.1 Internet access is provided to users for the performance and fulfillment of job responsibilities.

3.2 Employees should access Internet only through the connectivity provided by the bank and should not set up Internet access without authorization from IT department.

3.3 All access to Internet will be authenticated and will be restricted to business related sites.

3.4 Users are responsible for protecting their Internet account and password.

3.5 In case misuse of Internet access is detected, bank can terminate the user Internet account and take other disciplinary action as bank may deem fit.

3.6 Users should ensure that security is enabled on the Internet browser.

3.7 Users should ensure that they do not access websites by clicking on links provide in emails or in other websites.

3.8 Bank reserves the right to monitor and review Internet usage of users to ensure compliance to this policy.

3.9 The browser shall be patched with the latest patches whenever they are made available. User should also click on windows Update button periodically to check the patch status.

3.10 "Password save" button available under Auto-complete menu on the browser should be unchecked.

3.11 All the files downloaded from the Internet shall be screened with Gateway level AV and content Filter s/w.

4 E-mail Usage

Email Service

4.1 Use of Bank's official mail account for personal purposes is discouraged.

4.2 Users will be provided with a fixed amount of storage space in their mailboxes at the email server.

4.3 Bank does not maintain central or distributed electronic mail archives of all electronic mail sent or received.

4.4 The email message including all attached files will be limited to fixed size for transmission.

4.5 Personal email id which is not provided by the bank should not be used to send official communications.

Types of messages

4.6 Confidential or sensitive information should not be transmitted over email unless it is encrypted or password protected.

4.7 Emails that are not digitally signed should not be used for critical transactions requiring legal authentication of sender.

4.8 Users owning the email account are responsible for the content of email originated, replied or forwarded from their account to other users inside or outside the Bank

Account protection

4.9 Users should protect their email account on the server through strong password and should not share their password or account with anyone else.

4.10 Users should exercise caution in providing their email account or other information to websites or any other Internet forum like discussion board/ mailing list.

Monitoring & Reporting

4.11 Bank reserves the right to monitor email messages and may intercept or disclose or assist in intercepting or disclosing email communications to ensure that email usage is as per this policy.

4.12 Users should promptly report all suspected security vulnerabilities or incidents that they notice with the email system to the help desk or the branch / department system administrator.

5 Document and Storage Security

5.1 All documents containing sensitive information should be marked as "secret or confidential" both in electronic and print format.

5.2 All removable media including CD, floppy or DAT tape must be labeled as "secret or confidential" if it is used to store sensitive documents.

5.3 Confidential documents and media should not be kept unattended.

5.4 Users are encouraged to adopt a clean desk policy for papers, diskettes and other documentation.

5.5 Un-used documents/papers should be destroyed using shredder machine.

5.6 Users should keep a backup copy of important documents

Security of information

5.7 Sensitive information should not be discussed in the presence of external personnel or other Bank employees

5.8 Care should be exercised to protect sensitive information which may get revealed unintentionally due to unsafe practices.