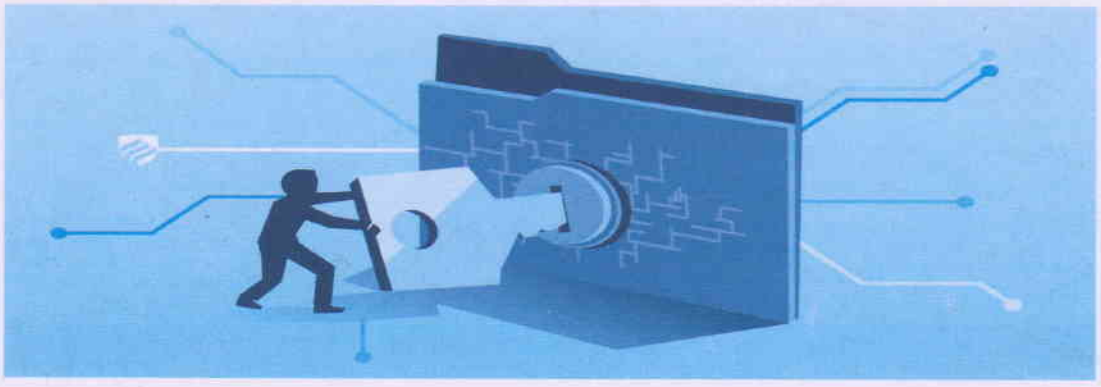
The Bihar State Co-operative Bank Ltd.

Ashok Rajpath, Patna – 800 004

Cyber Security Policy



CYBER SECURITY POLICY

INTENT:

It is the intent of this policy to establish guidelines for the employees using the Bank's computing facilities to access voice-mail, software, e-mail over the Internet, intranet access or any kind of networking used to connect with any link inside or outside the Bank.

PURPOSE:

Staff and officers using the internet or intranet facilities at The Bihar State Co-operative Bank Ltd.: These facilities are provided to employees for the purpose of conducting regular banking business. However, these facilities must be used responsibly by everyone, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt banking activities and interfere with the work or rights of others. Therefore, all employees are expected to exercise responsible and ethical behavior when using the Bank's internet and intranet facilities. Any action that may expose the Bank to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action and/or criminal prosecution.

POLICY:

The use of the Bank's internet or intranet facilities in connection with banking business and limited personal use is a privilege but not a right, extended to the Bank's employees. Users of The Bihar State Cooperative Bank Ltd.'s computing facilities are required to comply with all policies referred to in this document.

Users also agree to comply with applicable country, central, state, and local laws and to refrain from engaging in any activity that would subject the Bank to any liability. The Bihar State Cooperative Bank Ltd. reserves the right to amend these policies and practices at any time without prior notice and to take such further actions as may be necessary or appropriate to co applicable Central,
State / province, and local laws. To protect the integrity of The Bihar State Cooperative Bank Ltd's internet and intranet facilities and its users against unauthorized or improper use of those facilities, and to investigate possible use of those facilities in violation of Bank's rules and policies, The Bihar State Cooperative Bank Ltd. reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine the authorized use of any computing facility or which is used in violation of Bank's rules or policies. The Bihar State Cooperative Bank Ltd. also reserves the right periodically to examine any system and other usage and authorization history as necessary to protect its internet and intranet facilities.

SCOPE:

This policy applies to all The Bihar State Cooperative Bank Ltd. employees and affiliated societies. It is the responsibility of all operating units to ensure that these are clearly communicated, understood and followed. Policies also apply to software contractors, and vendors/suppliers providing services to The Bihar State Cooperative Bank Ltd. that bring them into contact with The Bihar State Cooperative Bank Ltd.'s Information Technology infrastructure. These policies cover the usage of all of the Bank's Information Technology and communication resources, including, but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, wireless computing devices, telecom equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected.

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

• All electronic communications equipment, including telephones, mobiles, radio communicators, voice-mail, e-mail, fax machines, wired or wireless communications devices and services, Internet and intranet and other on-line services.

• All software including purchased or licensed business software applications, Bank written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on Bank's-owned equipment.

• All intellectual property and other data stored on the Bank's equipment.

• All of the above are included whether they are owned or leased by the bank or are under the Bank's possession, custody, or control.

• These policies also apply to all users, whether on Bank's property, connected from remote via any networked connection, or using Bank's equipment.

CYBER SECURITY

1.INTRODUCTION

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information? The answer lies in cyber security.

Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days' cybercrimes are increasing day by day. Today more than 60percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. Even the latest technologies like cloud computing, mobile computing, Ecommerce, net banking etc also needs high level of security.

Since these technologies hold some important information regarding a person their security has become a must thing.

Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy.

The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information.

Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes.

2. CYBER CRIME

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime

May be defined as crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day-by-day technology is playing in major role in a person's life the cyber crimes also will increase along with the technological advances.

3.CYBER SECURITY

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

Policies on Cyber Security
of
The Bihar State Cooperative Bank Ltd.

1. Cyber Security Management.

a. The Board of Directors of the bank will be the ultimate decision maker in all internet or intranet facilities related activities.
b. The Board will be advised on matters related to internet or intranet facilities by a Computer Committee comprised of10to14 members selected from among Bank's officials and staffs.
c. other committees if felt necessary may be created by the Board of Directors on internet or intranet facility matters.

2. Cyber Security Record Management.

a. All available records of transactions and other related activities in a soft form will be maintained and stored live for a period of 10 years.
b. A data bank will be maintained to store records of transactions and other related activities conducted 10 years ago. This data bank will not be kept live but may be accessed as and when required and will be updated every financial year.
c. Data from this data bank will be having a system of uploading back to the live system if required, a resolution for which is to be passed and approved by the bank's Computer Committee.
d. Bank will ensure acquiring the latest technologies in the industry so that once acquired it lasts for at least the next five years.
e. All soft records of the bank will be audited periodically for their genuineness, integrity and authenticity.

3. Cyber Security Document Management

a. The bank will keep in custody and properly maintain all license related documents, which is to be kept under the purview of internal inspection.
b. All manuals and related documents will be managed under a library system.

4. Cyber Usage Policy

a. Acceptable Use

I. Running bank's implemented software
II. Conducting bank's day to day business activities
III. Using for other purpose suiting to the bank's needs
IV. Very limited personal use (Which cannot be considered as a right by any of bank's employees)

b. Inappropriate Use

I. Using internet or intranet facilities for personal use during transaction/business hours.
II. Unauthorized installing of any soft were whether license or pirated.
III. Using the internet or intranet facilities for recreational activities without proper authorization.
IV. Allowing unauthorized person to handle/ use bank's internet or intranet facilities.
V. Changing software/hardware/network settings without authorization

VI. Changing Software/Hardware / Network Configuration without authorization.

VII. Using the bank's internet or intranet facilities for malicious purposes like virus insemination, pornography, phishing, hacking, etc.

VIII. Any other use that is unethical and can be considered as detrimental to the interests of the Bank.

c. Penalties:

Any deviation from the above will result in the initiation of disciplinary action from the management of the bank.

5. Internet and E-mail Usage policy

a. Internet

I. The Bank's Computer Committee will advise on the user to whom an internet connectivity will be provided.

II. The node where such an internet connection is given will be separated by a firewall from bank's network.

III. Internet will be used for serving the purpose of the bank.

IV. No employee will download and install any software from the internet on bank's computer without prior and explicit permission.

V. Very limited personal use may be granted but cannot be considered as a right by any bank's employee.

VI. Internet will not be used for any unethical or malicious purpose.

b. E-mail

I. E-mail addresses will be assigned on bank's official website as per discretion of the management.

II. No e-mail will be sent using the bank's infrastructure that is detrimental to the functioning/image of the bank.

III. Communication that discloses personal information about Bank's Junk mail and chain letters are prohibited.

IV. Each employee is responsible for the content of all text, audio or images that he/she places on or sends over the bank's e-mail Internet or Intranet.

V. Employees may not hide their identities or represent that any email or other electronic communications were sent or receive from someone else.

VI. The use of instant messaging (IM) software such as AOL Instant messenger, Yahoo messenger or MSN Messenger is prohibited while connected to the bank's computer network explicit permission is granted.

6. Security

a. Bank will use industry recognized operating systems that are known to be strong against malwares such as viruses, in its servers/ nodes/ clients. e.g. – Unix, Linux, Windows etc.

b. will issue standard user ID to its employees from and above the rank of Grade III comprising of eight characters, of which the one Caps Alpha code, one numeric, and special character derived from the employee PF number issued to the employee from the bank's establishment section.

c. If an employee discloses his / her password to someone else, the employee may be held responsible for any activities of that other person while using that password.

d. Any employee of the bank logging into bank's system from any branch will do so only by using his/ her user identity and password.

e. The bank may monitor and inspect how any employee is using the bank's internet or intranet facilities, etc.

171

STATE CO-OPERATIVE BANK LTD. PATNA 1914

f. No employee may examine, change, use or delete any other person's file, output or user name without the other persons prior explicit permission (except for network administrators or other persons with management authorization acting in accordance with bank's policy).

7. Software Piracy (Software Piracy is a felony)

a. No program can be installed on more than one computer without multiply "Licenses" of some kind, with the exception of "Freeware "or in some cases "Shareware." If it does not say "Freeware" or "GPL" then it is not.
b. No employee shall bring any software from outside and install it on any of bank's computer.
c. No employee shall install any programs from one company computer to any other company computer without specific permission.
d. None of the bank's software is to be taken off site unless special permission is given.
e. No information about customer or the bank except in the form of a backup is to leave the building premises.

8. Inventory Management of Business IT Assets

a. BSCBs should maintain an up-to-date business IT Asset Inventory Register containing the following fields, as a minimum:
   I. Details of the IT Asset (viz., hardware/software/network devices, key personnel, services, etc.)
   II. Details of systems where customer data are stored
   III. Associated business applications, if any
   IV. Criticality of the IT asset (For example, High/Medium/Low)
b. Classify data/information based on sensitivity criteria of the information.
c. Appropriately manage and provide protection within and outside BSCB/network, keeping in mind how the data/information is stored, transmitted, processed, accessed and put to use within/outside the BSCB's network, and level of risk they are exposed to depending on the sensitivity of the data/information.

9) Environmental Controls

a. Put in place appropriate controls for securing physical location of critical assets (as identified by the Bank under its inventory of IT assets), providing protection from natural and man-made threats
b. Put in place mechanisms for monitoring of breaches/compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc. Appropriate physical security measures shall be taken to protect the critical assets of the Bank.

10) Network Management and Security

a. Ensure that all the network devices are configured appropriately and periodically assessed to ensure that such configurations are securely maintained.
b. The default passwords of all the network devices/systems should be changed after installation.
c. Put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.
d. Critical infrastructure of BSCB (viz., NEFT, RTGS, SWIFT, CBS, ATM infrastructure) should be designed with adequate network separation controls

STATE CO-OPERATIVE BANK LTD. PATNA 1914 BIHAR

11) Secure Configuration

a. The firewall configurations should be set to the highest security level and evaluation of critical device (such as firewall, network switches, security devices, etc.) configurations should be done periodically.
b. Systems such as Network, application, database and servers should be used dedicatedly for the purpose for which they have been set up.

12) Anti-virus and Patch Management

a. Put in place systems and processes to identify, track, manage and monitor the status of patches to servers, operating system and application software running at the systems used by the BSCB officials (end-users).
b. Implement and update antivirus protection for all servers and applicable end points preferably through a centralized system.

13) User Access Control / Management

a. Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a 'need to know' and 'need to do' basis.
b. Passwords should be set as complex and lengthy and users should not use same passwords for all the applications/systems/devices.
c. Remote Desktop Protocol (RDP) which allows others to access the computer remotely over a network or over the internet should be always disabled and should be enabled only with the approval of the authorized officer of the BSCB. Logs for such remote access shall be enabled and monitored for suspicious activities
d. Implement appropriate (e.g., centralized) systems and controls to allow, manage, log and monitor privileged/super user/administrative access to critical systems (servers/databases, applications, network devices etc.)

14) Secure mail and messaging systems

a. Implement secure mail and messaging systems, including those used by BSCB's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.
b. Document and implement email server specific controls.

15) Removable Media

a. As a default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorized for defined use and duration of use.
b. Secure the usage of removable media on workstations/PCs/Laptops, etc. and secure erasure/ deletion of data on such media after use.
c. Get the removable media scanned for malware/anti-virus prior to providing read/write access

16) User/Employee/Management Awareness

a. Communicate to users/employees, vendors & partner security policies covering secure and acceptable use of BSCB's network/assets including customer information/data, educating them about cyber security risks and protection measures at their level.
b. Conduct awareness/training for staff on basic information security controls (Do's and Don'ts), incident reporting, etc.

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914

c. Board members may be kept updated on basic tenets/principles of IT risk/cyber security risk at least once a year.
d. The end-users should be made aware to never open or download an email attachment from unknown sources

17) Customer Education and Awareness

a. Improve and maintain customer awareness and education with regard to cyber security risks.
b. Educate the customers on keeping their card, PIN etc. secure and not to share with any third party.

18) Backup and Restoration

Take periodic back up of the important data and store this data 'off line' (i.e., transferring important files to a storage device that can be detached from a computer/system after copying all the files).

19) Vendor/Outsourcing Risk Management

a. All the outsourcing service level agreements (SLAs) signed with the vendors must clearly mention the responsibility of the BSCB and vendor in case of any failure of services.
b. The agreements must clearly mention the grievance redressal mechanism to resolve customer complaints.
c. Vendors' service level agreements shall be periodically reviewed for performance in security controls.

This Policy has been approved by the Board of Directors of the Bank in its meeting held on dated 04.01.2022 with resolution no. 03

The management of the bank reserves the right to amend the policy at any point of time without prior notice.

BIHAR STATE CO-OPERATIVE BANK LTD. PATNA 1914