



दि अकोला अर्बन
को-ऑपरेटिव बँक लि; अकोला
(मल्टिस्टेट शोड्युलड बँक)

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) POLICIES

A Set of IT & IS Policies & Procedures



AU-ISMS-POL-L1-003

**Document Title: Information Security Management System (ISMS)
Policies**

Document Code: AU-ISMS-POL-L1-001

Document Type: Policy

Issued on: 15 March 2025

**Document Owner: Sunil V. Shejole, Head IT
Change Manager: Prashant Arbat, Prov. CISO**

Incident Manager: Sunil V. Shejole, Head IT

Change Priority: Medium


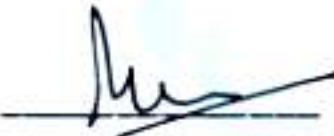
Document Classification: Internal



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिस्टेट रोडमुल बँक)

Review / Approval Matrix

	Prepared By	Reviewed By	Approved By
Name	Sunil V. Shejole, Head(IT)	Rajan Sontakke, CEO Prashant Arbat, CISO	The Board
Date	07 March 2025	13 March 2025	15 March 2025
Signature		 (CEO)  (CISO)	

Next Review Date: 31 March 2026

Distribution List

SN	Role/Designation
1	Board of Directors
2	Information Security Committee
3	All Staff and Managers
4	Any other entity authorized by the Board of Directors

© 2025 - Do not replicate/distribute without explicit written permission from the document owner.

INTERNAL AND CONFIDENTIAL

Page 1

THE AKOLA URBAN CO-OPRATIVE BANK LIMITED, AKOLA

INTERNAL DOCUMENT



I. Version History

Rev.	Revision Date	Change Description	Author	Reviewed By	Approved By
1.0	19/03/18	Initial Document	Sunil V. Shejole, Head(IT)	Rajan Sontakke, CEO	The Board
2.0	01/06/20	Major revision including the addition of several policies and structural revamp.	Sunil V. Shejole, Head(IT)	Rajan Sontakke, CEO	The Board
3.0	22/03/22	No Change	Sunil V. Shejole, Head(IT)	Rajan Sontakke, CEO	The Board
4.0	31/03/23	Change of Policy Template, Added NDU, AUP, Awareness Policy	Sunil V. Shejole, Head(IT)	Rajan Sontakke, CEO Prashant Arbat, Prov. CISO	The Board
4.0	07/03/24	No change	Sunil V. Shejole, Head (IT)	Rajan Sontakke, CEO Prashant Arbat, CISO	The Board
5.0	15/03/25	Added 19. Cryptographic Key Management Policy & 20. Teleworking Policy	Sunil V. Shejole, Head(IT)	Rajan Sontakke, CEO Prashant Arbat, CISO	The Board

॥ सहकारण जनकल्याणम् ॥



II. Abbreviations Used

Short Form	Abbreviations
The Bank	The Akola Urban Co-Operative Bank Ltd., Akola
AUCB	The Akola Urban Co-Operative Bank Ltd.
IT	Information Technology
IS	Information Security
ISMS	Information Security Management System
CIA	Confidentiality, Integrity, Availability
AUP	Acceptable Usage Policy
NDU	Non-Disclosure Understanding
ISSC	Information Systems Steering Committee
ISC	IS Committee * Same ISSC (Information Systems Steering Committee)
RBI	Reserve Bank of India
ESDS	Data Center vendor -ESDS Software Solution Limited
Virmati	CBS vendor - Virmati Software & Telecommunications Limited

॥ सहकारेण जनकल्याणम् ॥



III. Table of Contents

I. Review / Approval Matrix	1
II. Distribution List	1
III. Version History	2
IV. Revision Details for Version 4.0	2
V. Acronyms Used	3
VI. Table of Contents	4
VII. Introduction	6
VIII. Structure of this document	7
1. Version Control Policy	8
2. Acceptable Usage Policy	12
<i>Sample - Confidentiality and Non-Discloser Undertaking</i>	<i>15</i>
<i>Sample – Acceptable Usage Policy</i>	<i>18</i>
3. Logical Access Control Policy	22
3.1 Application Security Policy	23
3.2 Database Security Policy	28
3.3 Operating System Security Policy	32
3.4 Network Security Policy	39
3.5 E-Mail Security Policy	43
3.6 Internet Security Policy	47
3.7 Desktop and Laptop Security Policy	50
3.8 User Access Management Policy	53
3.9. Password Management Policy	57
4. Information Systems Outsourcing Policy	61
5. Internet Banking Security Policy	65
6. Mobile Banking Security Policy	70
7. Virus Protection Policy	73
8. Data Backup, Recovery and Retention Policy	79
9. Media Handling Policy	88
10. Change Management Policy	90
11. Security Incident Management Policy	93



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपटेट शेड्युलड बँक)

12. Log Management & Monitoring Policy	97
13. Personnel Security Policy	100
14. Physical and Environmental Security Policy	103
15. Business Continuity Management Policy	107
16. Asset Management Policy	109
17. Information Security Assurance Policy	113
18. Information Security Awareness Policy	115
19. Cryptographic Key Management Policy	119
20. Teleworking Policy	122
COPYRIGHT NOTICE	125

॥ सहकारेण जनकल्याणम् ॥

AUCB Helpdesk:

AUCB Helpdesk is an AUCB service desk tool which is used to raise service requests, requests for change (RFC), release tickets and problem tickets.

(AUCB Helpdesk Link: <https://help.aucbakola.com/>)



VII. Introduction

The banking industry uses information in every aspect of its business, from processing payments to making loan and investment decisions. Information and the supporting processes, the computer systems including networks and the human resources are important business assets of every Bank.

The use of Information Technology (IT) by banks and their constituents has grown rapidly and is now an integral part of the-operational strategies of banks. The Reserve Bank of India/ NABARD /NPCI etc, had, provided guidelines on Information Security, Electronic Banking, Technology Risk Management and cyber fraud. The measures suggested for implementation cannot be static and banks need to proactively create, fine-tune and modify their policies, procedures and technologies based on new developments and emerging concerns.

Since then, the use of technology by banks has gained further momentum. On the other hand, the number, frequency and impact of cyber incidents and attacks have increased manifold in the recent past, more so in the case of the financial sector including banks, underlining the urgent need to put in place robust cyber security and resilience framework at The Bank and to ensure adequate cyber security preparedness among banks on a continuous basis. In view of the low barriers to entry, evolving nature, growing scale/velocity, motivation and resourcefulness of cyber-threats to the banking system, it is essential to enhance the resilience of the banking system by improving the current defences in addressing cyber risks. These would include, but not be limited to, putting in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents or disruptions, if and when they occur. This will be ensured by capacity building. Further our bank will adhere to RBI's and other regulatory guidelines on the issue.

The Bank has recently migrated its' infrastructure to a reputed and leading Managed Data Center and Cloud Hosting Services Provider "**ESDS Software Solution Limited.**"; hereafter referred to as "**ESDS**". The ESDS is an ISO-27001:2013 and PCI-DSS-certified data center service provider with industries best technology and best practices. ESDS is responsible for managing Bank's IT Infrastructure and Network Services except for the Application maintenance services which continue to be the responsibility of the CBS vendor "**Virmati Software & Telecommunications Limited**" hereafter referred to as "**Virmati**". The Virmati is an established & renowned Software Technology Provider in Banking & Financial Industry, having partnered with Leading Financial Institutions & Business Associates over years.



An efficient Information Security (IS) framework is also a function of **awareness, knowledge** and **skills**.

- IT Governance entails several activities for the Board & Senior Management to become **aware** of and impact of IT on a bank.
- IT Security teams require **skills** and processes that are effective and needed to carry out efficient operations of the security policies.
- The people in the business functions (users of information and information assets) require **knowledge** on a day-to-day basis to use IT. For example, users at various levels in the bank should understand their role in very simple language like Do's and Don'ts; these are derived from the Policy Statement(s).

VIII. Structure of this document

This document is divided into various sections and is structured as under

- **Objectives:** This section states the purpose of the policy.
- **Policy Scope:** This section defines various internal and external entities as well as the Information Assets to which that policy statement/s applies.
- **Policy Statement(s):** This section describes the Information Security Policies of The Bank for each control area.
- **Procedures:** This section describes the Information Security Procedures to comply with the Security Policy. However, this section does not describe the Technical and/or procedural details to implement these Procedures.
- **Responsibilities:** This section describes the entities that are generally responsible for the implementation of information security policies for a given area.

॥ सहकारेण जनकल्याणम् ॥

<< Space intentionally left blank >>



1. Version Control Policy

Objective

The purpose of this policy is to maintain the integrity and usage of only to keep a clear record of how the document was created, developed and changed over time by The Banks staff, members and all other stakeholders.

Scope

This policy covers all to ensure the accuracy and integrity of all documentation uses current and approved documentation.

Policy Statement(s)

- Version numbering system:** Establish a consistent system for numbering versions of documents. This can include a combination of letters and numbers, such as V1.0, V1.1, V2.0, etc.
- Revision history:** Keep a record of all changes made to a document, including the date, version number, and a brief description of the changes.
- Approval process:** Define the process for approving new versions of documents. This can include a review by a designated team or individual, and a sign-off process for final approval.
- Distribution process:** Define how documents will be distributed to stakeholders, including the format (digital or hard copy) and the frequency of distribution.
- Archiving process:** Establish a process for archiving older versions of documents. This can include a timeline for archiving, and a designated location for storing archived documents.
- Access control:** Define who has access to different versions of documents, and how access is granted and revoked. This can include password-protected folders or a document management system with user permissions.
- Communication plan:** Develop a plan for communicating changes to documents and new versions to stakeholders. This can include email notifications, a newsletter, or a company-wide announcement.

Procedures

N	Procedures
1.	Creating/reviewing documents
	<ul style="list-style-type: none">All Managers & Department Coordinators initiate the review or the development of documents not limited to policies, procedures, processes and forms required for their department.



	<ul style="list-style-type: none">• All Managers and Department Coordinators will liaise with IT Manager while creating a new required document or reviewing the existing document.• The relevant regulatory guidelines and/ or other relevant sources of information are checked to ensure the document meets the compliance requirements.• A document versioning policy should include document sensitivity information such as confidential, internal, and public, to ensure appropriate protection and accessibility of documents.• The manager changes the version number of the documents as per version control protocol and shares it back with relevant stakeholders to confirm the contents and integrity of the document.• The finalised document will be presented to concerned Boards and Committees for endorsement as per their alignment. However, in any case, the amended documents will be updated in the Management Meeting, endorsed and recorded in the minutes.• Once the document has been approved it is then saved in the relevant folder in the system and notified to the relevant staff members for use only from there.• All documents that have gone through the Version control process must include information to indicate this.<ul style="list-style-type: none">➤ The Bank's logo and statements must be deployed on all documentation where appropriate and in accordance with usage guidelines.➤ The details of each document must reflect the version number, title of a document, approved by, version number and date.• When a document is created or amended the document register must be updated.
2. Storing documents	
	<ul style="list-style-type: none">• Once a document has been created/ amended and approved by the IT Manager it must be then placed in the appropriate version control folder for use.• The version control folders are located over the network.• The new document must be placed in the current Version control folder over the network.• The old versions must be placed in the archive folder.• A maximum of three old versions are maintained in each archive folder.• Under no circumstances should staff use documents placed in the archive folder.• Only the Executive Management or personnel authorised by him/her can place/ remove documents from the version control folder.• A word and PDF version of each document is maintained.• All documents are backed up regularly and also stored on and off-site.



3.	Accessing documents
	<ul style="list-style-type: none">• All staff only access documents from the version control file management system on the network.• When printing documents only access documents from the version control file management system on the network.• Check to ensure the document is the current version before utilisation.• The document register contained in the version control file management system will indicate the current version.• Protected PDF versions are to be used when printing• Only keep drafts of documents if it is also important to keep a record (audit trail) of the process, decision making or context, in which the formulation of the document/file took place. There may be business requirements to do so. Although documents are superseded by a later final version, remember it may also be important for The Bank to retain older versions of a document, for instance, to demonstrate what policy, regulation or condition of the grant was “in force” at a particular time.
4.	Installations and Configurations
	<p>Only the IT department / designated users shall carry out any installations and configurations.</p> <p>Users shall not add, modify or remove any system hardware and/or software component on the IT system provided by The Bank.</p>
5.	Nomenclature
	<p>Method 1: Tracking Version Numbers</p> <p>Below is the standardisation nomenclature that can be used for the Policy, Procedure Guidelines etc. documents.</p> <p>AU-ISMS-POL-L1-001</p> <p>1 2 3 4 5</p> <p>1 → Abbreviation for the Akola Urban</p> <p>2 → Short form/abbreviation of the Department or Subject (2 or 4 Characters) e.g. IT, IS, ISMS, BCMS, HRMD, FRMS etc.</p> <p>3 → Type of Document POL: Policy STD: Standard</p>



	<p>GID: Guideline PRO: Procedure</p> <p>4 → Level of the Document L1: Level 1 (Staff Level) L2: Level-2 (Supervisory/Managerial Level) L3: Level-3 (Management/Executive Level)</p> <p>5 → Unique number to the document for identification (3 Digits)</p> <p>Method 2: Tracking Version Numbers Numbering each version helps to distinguish one version from another. It may be suitable, simply to number each version, regardless of the changes, using consecutive whole numbers e.g. V 1.0; V 2.0; V 3.0 etc. to track which version of the document is being worked on. Where it is important to identify and track minor or major revisions to the document, before a final version is agreed upon, then a more formal numbering system may be required. Minor revisions would indicate where small changes have been made to the document such as spelling or grammar corrections, or where changes have been made that do not require further approval. Minor revisions are indicated by making increments to the decimal place e.g. V 1.2; V 1.3; V1.4 etc.</p> <p>Method 3: Use File Naming Conventions Use the file name to simply identify the version and status of the document, along with the topic e.g. DataProtectionPolicy_Draft_V1.0 DataProtectPolicy_Revision_V1.1DataProtectionPolicy_Final_V2.0</p>
6. Document Review	
	<ul style="list-style-type: none">• All documents are reviewed at least annually through the Continuous Improvement Policy and procedure.• Amendments are implemented in accordance with this policy and procedure.• This policy and procedure are reviewed annually as part of the Continuous improvement policy and procedure.

Responsibilities

- Manager-IT
- Administration department
- All Managers and Department Coordinators

xxxxxx End of Policy Documents xxxxxx



2. Acceptable Usage Policy

Objective

The objective of this policy is to outline the acceptable use of computer equipment and information assets at The Bank. These rules are in place to protect the users and The Bank. Inappropriate use may expose The Bank to risks including virus attacks, compromise of network systems and services and legal issues.

Scope

This policy covers all information assets and all users of The Bank.

Policy Statement(s)

1. System Usage: - Information assets shall be used for official purposes only
2. Responsibility of Users: - Every computer user shall know, understand and adhere to the Information Security Policies and Procedures
3. Limited personal use: - Users may use The Bank's information assets for limited personal usage prudently and ensure that it does not produce hindrance to the functionality or is not conflict with The Bank's policies
4. Installation and Configuration: - Users shall not add, modify or remove any system hardware and/or software component on the IT system provided by The Bank
5. Compliance with this policy is mandatory
6. Users shall take reasonable measures to protect the equipment from damage, theft or loss

Procedures

SN	Procedures
1.	System Usage
	Internet / Extranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts, electronic mail, Internet browsing, FTP, etc. are the property of The Bank. These information assets are to be used for business purposes to serve The Bank operations and its users in the course of normal operations.
2.	Responsibility of Users
	Effective security is a team effort involving the participation and support of every user who deals with information and/or information processing systems of The Bank.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपेटिट शेड्युलड बँक)

SN	Procedures
	It is the responsibility of every computer user to know, understand and adhere to the Information Security Policies and Procedures defined in this document.
3.	Personal usage of the information assets provide to the users
	<p>Users are given access to various information assets of The Bank, like Computer Desktops/Laptops, e-mail facilities, Internet facilities, etc. to help them perform their day-to-day operations.</p> <p>Although these Information Assets are to be used for Business Purposes only, the management appreciates that the users may use these Information Assets for limited personal usage e.g. the users may store a reasonable amount of personal data on The Bank's assets, as far as it does not produce hindrance to the functionality or is not conflicting with The Bank's policies, OR users may be allowed to access the internet to view their e-mails etc.</p> <p>While the Management desires to provide a reasonable level of privacy, users should be aware that any personal data they create / copy on the corporate systems, remains the property of The Bank.</p> <p>It is the responsibility of every user to read and understand the "Information Security Procedures" as defined by The Bank from time to time and ensure complete and unconditional adherence.</p> <p>The Management cannot define "reasonable usage" and it is the responsibility of each user to ensure that such usage is prudent, really limited and does not affect his / her job performance. The final authority to define "reasonable personal usage" rests with the management, which may be decided on a case-to-case basis.</p> <p>Appropriate disciplinary actions will be initiated against those users, who violate the "prudent personal usage" of information assets provided by The Bank.</p>
4.	Installations and Configurations
	<p>Only the IT department / designated users shall carry out any installations and configurations.</p> <p>Users shall not add, modify or remove any system hardware and/or software component on the IT system provided by The Bank.</p>
7.	Compliance
	<p>The Bank reserves its' right to audit networks and systems on a periodic basis to ensure compliance with this policy without any notice to the users.</p>
8.	Equipment Protection
	<p>Users shall take reasonable measures to protect the equipment from damage, theft or loss.</p>



Responsibilities

- IT Support Team
- Departmental Heads
- All users of The Bank

<< Space intentionally left blank >>

॥ सहकारेण जनकल्याणम् ॥



Sample - Confidentiality and Non-Disclosure Undertaking

Sr.No.R«SrNo»

कर्मचारी गोपनीयता आणि गैर प्रकटीकरण-वचन

EMPLOYEE CONFIDENTIALITY AND NON-DISCLOSURE UNDERTAKING

हा वचननामा दिनांक _____, श्रीश्रीमती/सौ/, «□□□□□□□□□□□□□□□□» (यापुढे, "कर्मचारी यांच्या ("लेखी संमतीनुसार अंमलात आला. (THIS UNDERTAKING is entered into as of _____ ("Effective Date"), Mr./Mrs/Miss, «Emp_Name» (hereinafter, the "Employee").)

जेव्हा, बँक आणि कर्मचारी कर्मचाऱ्यांसाठी बँकेसाठी सेवा करण्यासाठी सदर (यापुढे संदर्भितपक्ष) वचननामा करीत आहेत ज्यासाठी बँकेला गोपनीय आणि मालकीची माहिती कर्मचाऱ्यांना उघड करणे आवश्यक असू ("गोपनीय माहिती") शकते. म्हणूनच, येथे खाली लिहिलेल्या वाचलेल्या वचनांचा विचार करून /, प्रत्येक संदर्भितपक्ष खालील तरतुदींशी सुसंगतपणे लागू होणारी माहिती उघड करण्यास आणि प्राप्त करण्यास सहमत आहे. (WHEREAS, the Bank and the Employee (hereinafter referred to as the party and/or the parties) are entering into an arrangement for Employee to perform services for Bank which may require Bank to disclose confidential and proprietary information ("Confidential Information ") to Employee; NOW, THEREFORE, in consideration of the promises recited herein, each party hereto agrees to disclose and to receive information as applicable in a manner consistent with the following provisions:)

१ म्हणजे कोणतीही "गोपनीय माहिती" आणि सर्व माहिती, माहिती आणि डेटा, तांत्रिक किंवा गैरतांत्रिक-, किंवा बँक, बँकेचा व्यवसाय किंवा व्यवहार आणि किंवा कर्मचाऱ्यांच्या सेवांना प्रभावित करणाऱ्या किंवा त्यांच्याशी संबंधित कोणत्याही बाबींचे / वर्णन, बँकेची उत्पादने, रेखाचित्रे, योजना, प्रक्रिया किंवा इतर डेटा बँकेने कर्मचाऱ्याला उघड केला आहे किंवा प्रदान केला आहे, तो तोंडी, लेखी, चित्र, छायाचित्र, इलेक्ट्रॉनिक किंवा इतर कोणत्याही स्वरूपात खुलासा किंवा प्रदान केला असला तरीही. ("Confidential Information" shall mean any and all information, know-how and data, technical or non-technical, or description concerning any matters affecting or relating to Employee's services for Bank, the business or operations of Bank, and/or the products, drawings, plans, processes, or other data of Bank disclosed or provided by Bank to the Employee, whether disclosed or provided in oral, written, graphic, photographic, electronic or any other form.)

२ कर्मचारी खालील नियम व अट स्विकारून सही करण्यास सहमत आहेत. (The Employee agrees to:)

- बँकेकडून मिळालेली गोपनीय माहिती काटेकोरपणे विश्वासात ठेवावी आणि इतरांसमोर उघड होऊ नये यासाठी योग्य प्रमाणात योग्य काळजी घ्यावी; (Hold the Confidential Information received from Bank in strict confidence and shall exercise a reasonable degree of care to prevent disclosure to others;)
- बँकेला प्रथम अधिकृत केल्याशिवाय गोपनीय माहिती प्रत्यक्ष किंवा अप्रत्यक्षपणे इतरांना उघड किंवा प्रसिद्ध करणार नाही. (Not disclose or divulge either directly or indirectly the Confidential Information to others unless first authorized to do so by Bank.)
- कर्मचारी गोपनीय माहितीचे प्रतिलिपि पुनरुत्पादन करणार नाही किंवा या माहितीचा वापर व्यवसायिकरित्या / तिची कर्तव्ये पार पाडण्याव्यतिरिक्त इतर कोणत्याही हेतूसाठी करणार / करणार नाही केवळ बँकेसाठी त्याच्या नाही. (Employee will not reproduce the Confidential Information nor use this information commercially or for any purpose other than the performance of his/her duties for Bank.)
- कर्मचारी, विनंती केल्यावर किंवा बँकेशी असलेले त्याचे तिचे नाते संपुष्टात आल्यानंतर, बँकेकडून प्राप्त झालेले किंवा बँकेसाठीच्या उपक्रमांमधून आलेले कोणतेही रेखाचित्र, नोट्स, दस्तऐवज, उपकरणे आणि आदि साहित्य बँकेलाच सुपूर्द करेल. (Employee will, upon the request or upon termination of his/her relationship with Bank, deliver to Bank any drawings, notes, documents, equipment, and materials received from Bank or originating from its activities for Bank.)

३ कर्मचाऱ्यांकडून प्राप्त झालेल्या कोणत्याही माहितीचा भाग किंवा प्रकल्प विशिष्ट व्यवहार ठरवण्याचा एकमेव अधिकार बँकेला असेल, ज्यात व्यापारिक गुपित ट्रेड) सीक्रेट ठेवण्याच्या अधिकारा (सह, पूर्व पेटंट अर्जाशिवाय, प्रकाशन अधिकार स्वतःच्या नावाने वापरण्याचा आणि उघड करण्याचा अधिकार असेल किंवा बँकेला योग्य वाटेल त्याप्रमाणे इतर कोणत्याही



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपेटिट शेड्युलड बँक)

प्रक्रियेचे पालन करणे असेल. (Bank shall have the sole right to determine the treatment of any information that is a part or project specific received from Employee, including the right to keep the same as a trade secret, to use and disclose the same without prior patent applications, to file copyright registrations in its own name or to follow any other procedure as Bank may deem appropriate.)

४ गोपनीय माहितीच्या . वापरामुळे उद्भवलेली कोणतीही माहिती, घडामोडी, शोध, तंत्रज्ञान, आविष्कार आणि यासारख्या गोष्टींचा दावा करणारे कोणतेही पेटंट अर्ज दाखल न करण्यास मी कर्मचारी म्हणून सहमत आहे किंवा जी गोपनीय माहितीच्या अभावी बनवली, विकसित किंवा शोधली जाऊ शकली नसती. (I am beaing the Employee agrees not to file any patent applications claiming any information, developments, discoveries, technologies, inventions and the like arising from the use of Confidential Information or that could not have been made, developed or discovered but for access to Confidential Information.)

५ सक्षम अधिकार क्षेत्राच्या कोणत्याही न्यायालयाने नंतर या .वचननाम्यातील कोणत्याही तरतुदी अवैध, बेकायदेशीर किंवा लागू न करण्यायोग्य असल्याचे मानले तर, अशा तरतुदी या वचननाम्यातून खंडित केल्या जातील इतर सर्व तरतुदी ., अधिकार आणि दायित्वे खंडित केलेल्या तरतुदीकडे दुर्लक्ष करून चालू राहतील आणि या वचननाम्याच्या उर्वरित तरतुदी प्रत्येक पक्षांच्या हेतूनुसार असतील. (Should any court of competent jurisdiction later consider any provisions of this Undertaking to be invalid, illegal, or unenforceable, such provisions shall be considered severed from this Undertaking. All other provisions, rights, and obligations shall continue without regard to the severed provision, provided that the remaining provisions of this Undertaking are in accordance with the intentions of the parties.)

६ कोणत्याही विशिष्ट कालावधीसाठी सतत रोजगाराचे वचन म्हणून या .वचननाम्याचा काहीही अर्थ लावला जाणार नाही. (Nothing in this Undertaking shall be construed as a promise of continued employment for any specific period of time.)

७ या .वचननाम्यातील कोणतीही गोष्ट कर्मचाऱ्यांच्या रोजगाराच्या 'इच्छेनुसार' स्वरूप बदलत नाही किंवा बदलत नाही. (Nothing in this Undertaking modifies or alters the 'at-will' nature of employee's employment.)

८. या वचननाम्याचे उल्लंघन केल्यास मला/कर्मचाऱ्याला बँकेच्या शिस्तपालन धोरणानुसार सेवासंपुष्टात येईपर्यंत प्रशासकीय शिस्तभंगाची कारवाई होऊ शकते. (Violation of this Undertaking will subject I/Employee to disciplinary action according to Employer's disciplinary policy, up to and including termination.)

प्रतिज्ञापत्र

(Solemn affirmation)

दि अकोला अर्बन को-ऑपरेटिव्ह बँक, लि., अकोला, चे, मी वरीलप्रमाणे सारांशित केलेले धोरण वाचले आहे आणि त्यातील मजकूर आणि ईतर संबंधित धोरणांच्या अटींचे पालन करण्यास सहमती दर्शविली आहे. तसेच उपरोक्त प्रमाणे, मला माहिती प्रणाली सुरक्षा, सायबर सुरक्षा, वैयक्तिक माहिती संरक्षण (डेटा प्रायव्हसी) आणि संस्थेच्या अन्य धोरणा संबंधित वेळोवेळी जागरूक करू शकते. (I have read the policy summarized above and agree to abide by its contents and the terms of other related policies. The Akola Urban Co-operative Bank, Ltd., Akola may make me aware from time to time regarding information system security, cyber security, protection of personal information (data privacy) and other policies of the organization. I have read the policy summarized above and agreed to comply with its contents and any other relevant policies of which the organization may make me aware related to the information security personal data protection policy.)

मान्यतेसाठी ACCEPTED:

वापरकर्त्याचे नाव : «कर्मचार्याचे_नाव»

Name of User : «Emp_Name»

वापरकर्त्याचा हुद्दा : «पदनाम»

Designation of User : «Designation»

वापरकर्त्याची स्वाक्षरी: _____

Signature of User: _____

Date:

तारीख:

Place : «BRNAME»

स्थळ : «शाखेचे_नाव»



Sample – Acceptable Usage Policy

ACCEPTABLE USAGE POLICY (AUP))स्वीकाराई वापर धोरण(

This Acceptable Use Policy covers the security and use of all The Akola Urban Co-operative Bank, Ltd., Akola information, computer and system equipment. It also includes email, internet, voice, mobile and IT equipment etc. This policy applies to all The Akola Urban Co-operative Bank, Akola employees, contractors and agents.)हे स्वीकाराई वापर धोरण सर्व दि अकोला अर्बन कोऑपरेटिव बँक, लि., अकोला माहिती, संगणकाचा आणि सिस्टमच्या उपकरणांची सुरक्षा आणि वापर यांनासमाविष्ट करतेयात ईमेल, इंटरनेट, व्हॉईस, मोबाइल आणि आयटी उपकरणे इत्यादीयांचाही समावेश आहे-हे धोरण सर्व दि अकोला अर्बन को ऑपरेटिव बँक, अकोला चे कर्मचारी, कंत्राटदार आणि एजंट यांना लागू होते(.

Please ensure you have read the following summary of the main points of the organization's policies with regard to information security.)कृपया माहिती सुरक्षिततेच्या संदर्भात संस्थेच्या धोरणांच्या मुख्य मुद्द्यांचा खालील सारांश तुम्ही वाचला असल्याची खात्री करा(.

1. I acknowledge that my use of the organization's computer and systems may be monitored and/or recorded for lawful purposes.(मी कबूल करतो की माझ्या संस्थेच्या संगणकाचा आणि सिस्टमच्या वापराचे परीक्षण केले जाऊ शकते आणि किंवा / (कायदेशीर हेतूसाठी रेकॉर्ड केले जाऊ शकते
2. I accept that I am responsible for the use and protection of the user credentials with which I am provided (user account and password, access token or other items I may be provided with).(मी स्वीकार करतो की मला प्रदान केलेल्या वापरणाऱ्याचे खाते व पासवर्ड (क्रेडेन्शियल्सच्या वापरकर्ता खाते आणि पासवर्ड) वापरासाठी आणि संरक्षणासाठी मी जबाबदार आहे (, प्रवेश टोकन किंवा मला प्रदान केलेल्या इतर बाबी(.
3. I will not use anyone else's user account and password to access company systems.(संस्थेच्या सिस्टममध्ये प्रवेश करण्यासाठी मी इतर कोणाचेही वापरकर्ता खाते आणि पासवर्ड वापरणार नाही(.
4. I will not attempt to access any computer system to which I am not been given access.) मी कोणत्याही संगणक प्रणालीमध्ये प्रवेश करण्याचा प्रयत्न करणार नाही ज्यामध्ये मला प्रवेश दिला गेला नाही(.
5. I will protect any classified material sent, received, stored or processed by me according to the level of classification assigned to it, including both electronic and paper copies.) इलेक्ट्रॉनिक आणि कागदी दोन्ही प्रतींसह, त्याला नियुक्त केलेल्या वर्गीकरणाच्या पातळीनुसार माझ्याद्वारे पाठवलेल्या, प्राप्त झालेल्या, संग्रहित केलेल्या किंवा प्रक्रिया केलेल्या कोणत्याही वर्गीकृत सामग्रीचे मी संरक्षण करीन(.
6. I will ensure that I label any classified material that I create appropriately according to published guidelines so that it remains appropriately protected.)मी हे सुनिश्चित करेन की मी प्रकाशित केलेल्या मार्गदर्शक तत्वांनुसार मी तयार केलेली कोणतीही वर्गीकृत सामग्री योग्यरित्या लेबल करेन की जेणेकरून ती योग्यरित्या संरक्षित राहील(.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपेटिट शेड्युलड बँक)

7. I will not send confidential information over the Internet unless appropriate methods (e.g. encryption or password protection) have been used to protect it from unauthorized access. (अनाधिकृत प्रवेशापासून संरक्षित करण्यासाठी योग्य पद्धती वापरल्यास (एनक्रिप्शन किंवा पासवर्ड संरक्षण, उदा) विषय मी इंटरनेटवरून गोपनीय माहिती पाठवणार नाही.)
8. I will always ensure that I enter the correct recipient's email address(es) so that confidential information is not compromised. (मी नेहमी खात्री करून की मी योग्य प्राप्तकर्त्याचा ईमेल पत्ता प्रविष्ट केला आहे जेणेकरून गोपनीय माहितीशी तडजोड होणार नाही.)
9. I will ensure I am not overlooked by unauthorized people when working and will take appropriate care when printing confidential information. (मी काम करताना अनधिकृत लोकांकडून /माझ्याकडून दुर्लक्ष होणार नाही याची खात्री करीन आणि गोपनीय माहिती छापताना योग्य ती काळजी घेईन.)
10. I will securely store confidential printed material and ensure it is correctly destroyed when no longer needed. (मी गोपनीय मुद्रित सामग्री सुरक्षितपणे संग्रहित करीन आणि जेव्हा यापुढे गरज नसेल तेव्हा ती योग्यरित्या नष्ट केली जाईल याची खात्री करेन.)
11. I will not leave my computer unattended so that unauthorized access to information via my account is prevented while I am away. (मी माझा संगणक दुर्लक्षित ठेवणार नाही जेणेकरून मी दूर असताना माझ्या खात्याद्वारे माहितीवर अनधिकृत प्रवेश प्रतिबंधित केला जाईल.)
12. I will make myself familiar with the organization's security policies and procedures and any special instructions relating to my work. (मी स्वतःला संस्थेची सुरक्षा धोरणे आणि कार्यपद्धती आणि माझ्या कामाशी संबंधित कोणत्याही विशेष सूचनांशी परिचित करून देईन.)
13. I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security or if I observe any suspected information security weaknesses in systems or processes. (मी सुरक्षेचा भंग करणारी एखादी घटना आढळल्यास, संशयित किंवा साक्षीदार दिसल्यास किंवा सिस्टम किंवा प्रक्रियांमध्ये मला माहिती सुरक्षा कमकुवतपणा आढळल्यास ताबडतोब माझ्या व्यवस्थापक, आयटी विभाग, माहिती सुरक्षा विभाग किंवा संगणक मदत कक्षाला विलंब न करता कळवणे ही माझी जबाबदारी आहे.)
14. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than the intended purpose. (मी सिस्टीम सुरक्षा नियंत्रणे प्रतिरोध किंवा विस्कळीत करण्याचा प्रयत्न करणार नाही किंवा इच्छित उद्देशाव्यतिरिक्त इतर कोणत्याही हेतूसाठी वापरणार नाही.)
15. I will not remove equipment or information from the organization's premises without appropriate approval. (मी योग्य मंजूरीशिवाय संस्थेच्या परिसरातून उपकरणे किंवा माहिती काढणार नाही.)
16. I will permit my personal mobile number and devices to use them for organizational transactions and will not connect them to the computer system and network without the approval of the organization. (मी मान्य करतो की, बँकेच्या मंजूरी शिवाय माझी वैयक्तिक मोबाइल क्रमांक आणि उपकरणे ही संस्थेच्या संगणक सिस्टम आणि नेटवर्कला जोडणार नाही आणि त्यांचा बँकेच्या व्यवहारासाठी वापर करण्यास माझी परवानगी असेल.)
17. I will take precautions to protect all computer media and mobile devices when carrying them outside my organization's premises (e.g. not leaving a laptop unattended or on the public display



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेट शैड्युलड बँक)

such that it would encourage an opportunist theft). (मी सर्व संगणक माध्यमे आणि मोबाईल उपकरणे माझ्या संस्थेच्या आवाराबाहेर घेऊन जाताना सुरक्षित ठेवण्यासाठी खबरदारी घेईन लॅपटॉप दुर्लक्षित न ठेवता किंवा सार्वजनिक प्रदर्शनावर अशा प्रकारे ठेवू नका की यामुळे संधीसाधू .उदा) .चोरीला प्रोत्साहन मिळेल

18. I will not introduce viruses or other malware into the system or network. (मीसिस्टम किंवा नेटवर्कमध्ये व्हायरस किंवा इतर मालवेअर सॉफ्टवेअरआणणार नाही).
19. I will not attempt to disable the anti-virus protection provided on my computer. (मी माझ्या संगणकावर प्रदान केलेले अँटी व्हायरस संरक्षण-व्यत्यय किंवा बंद करण्याचा प्रयत्न करणार नाही).
20. I will comply with the legal, statutory or contractual obligations that are relevant to my role. (मी माझ्या भूमिकेशी संबंधित असलेल्या कायदेशीर, वैधानिक किंवा वचननामाच्या दायित्वांचे पालन करीन).
21. On leaving the organization, I will inform my manager prior to my departure of any important information held in my account, and facilitate the removal of all access granted to me relevant to my previous role. (संस्था सोडताना, माझ्या खात्यात असलेली कोणतीही महत्वाची माहिती मी माझ्या खात्यातून बाहेर पडण्यापूर्वी माझ्या व्यवस्थापकाला कळवीन आणि माझ्या पूर्वीच्या भूमिकेशी संबंधित मला दिलेले सर्व प्रवेश काढून टाकण्याची सोय करेन).

DECLARATION घोषणापत्र

I have read the policy summarized above and agree to abide by its contents and the terms of other related policies. The Akola Urban Co-operative Bank, Ltd., Akola may make me aware from time to time regarding information system security, cyber security, protection of personal information (data privacy) and other policies of the organization. I have read the policy summarized above and agreed to comply with its contents and any other relevant policies of which the organization may make me aware related to the information security / personal data protection policy. (मी वरीलप्रमाणे सारांशित केलेले धोरण वाचले आहे आणि त्यातील मजकूर आणि ईतर संबंधित धोरणांच्या अटींचे पालन करण्यास सहमती दर्शविली आहेओपरेटीव्ह बँक-दि अकोला अर्बन को ., लि., अकोला मला माहिती प्रणाली सुरक्षा, सायबर सुरक्षा, वैयक्तिक माहिती संरक्षण (डेटा प्रायव्हसी)आणि संस्थेच्या अन्य धोरणा संबंधित वेळोवेळी जागरूक करू शकते).

वापरकर्त्याचे नाव :«कर्मचार्याचे_नाव»

Name of User :«Emp_Name»

वापरकर्त्याचा हुद्दा :«पदनाम»

Designation of User :«Designation»

वापरकर्त्याची स्वाक्षरी: _____

Signature of User: _____

Date:

तारीख:

Place :«BRNAME»

स्थळ :«शाखेचे_नाव»

xxxx End of Policy Documents xxxxxx



3. Logical Access Control Policy

Objectives

The objective of this policy is to establish controls on accessing the logical assets of The Bank such as Operating Systems, Databases, Network Devices etc.

Scope

This policy covers all information assets and all users of The Bank.

Policy Statement(s)

1. Logical access controls should be established for applications.
2. Logical access controls should be established for the databases.
3. Logical access controls should be established for operating systems.
4. Logical access controls should be established for network devices.
5. Logical access controls should be established for the E-Mail system.
6. Logical access controls should be established for Internet access.
7. Logical access controls should be established for desktops and laptops.
8. Logical access controls should be enforced via user access management.
9. Adequate password management controls should be established

Procedures

This is the primary policy that contains a subset of policies and procedures which addresses Logical Access Controls.

The subset policies are as below:

- 3.1 Application Security Policy
- 3.2 Database Security Policy
- 3.3 Operating System Security Policy
- 3.4 Network Security Policy
- 3.5 E-Mail Security Policy
- 3.6 Internet Security Policy
- 3.7 Desktop and Laptop Security Policy
- 3.8 User Access Management Policy
- 3.9 Password Management Policy



3.1 Application Security Policy

Objectives

The Application Security Policy is designed to ensure that

- The application should meet the business and user requirements.
- The application should comply with various security requirements like authentication, authorisation and auditing controls.
- The Application should help ensure non-repudiation of any transactions done by the users.
- Adequate controls are built into the Application software to prevent loss, modification or misuse of data.
- The production environment is adequately segregated from the Test and development environments.
- Changes to the Application systems are controlled and are done as per the change management policy.
- The application generates adequate and secure audit trails to help establish accountability.

Scope

This policy is applicable to all Applications installed and used within The Bank environment and is applicable to all users including employees, contractors, consultants, and temporary users.

Policy Statement(s)

1. The application owner should be identified.
2. The administrator of each Application shall be identified and the roles and responsibilities shall be defined, documented and communicated
3. Up-to-date Inventory of the Applications shall be maintained
4. Ensure safe custody of installation kits for applications owned by them
5. Only those components in applications which are necessary for the business shall be installed
6. Procedures shall be established for ensuring the integrity of the systems
7. Appropriate Input, Process and Output controls shall be defined, designed, developed, implemented and tested
8. Controls over interfaces and intermediate Files shall be established
9. Applications accessible over the internet shall be duly secured
10. Maker – Checker Controls over Inputs shall be established
11. Each application shall be tested for business functionality and security before being moved into the production environment



12. Scripts which are developed outside of the Application for additional functionality shall be tested, documented and integrity control maintained
13. Procedures shall be established for User Access Management Controls
14. Procedures shall be established for Password Management Controls
15. Procedures shall be established for Log Management Controls
16. Procedures shall be established for Change Management Controls
17. Procedures shall be established for Security Incident Management Controls
18. Procedures shall be established for Data Backup, Recovery and Retention Policy Controls

Procedures

SN	Procedures
1.	Application Ownership
	<ul style="list-style-type: none">The Business In-charge will be the owner of Business Applications and shall be responsible for the confidentiality, integrity and availability of the Application. E.g. the Owner of the Core Banking Application would be the Head of banking operations, Owner of the HRMS Application would be the Head of the HR Department. In the case of shared Applications like E-Mail, the IT Manager will be the ownerAlthough the Business Owner will be non-technical, he will still be responsible for the security of the Application and infrastructure supporting the Business Application e.g. Operating System, Database, Web Server, Firewall etc. He will take the necessary support and guidance from the IT Manager.The application owner will be also ensuring that Application Security Procedure as mentioned below is implemented
2.	The Administrator – Roles and Responsibilities
	<p>The administration of the Application should be identified and the roles and responsibilities should be defined, documented and communicated.</p> <p>The administrator should be given adequate training on the roles and responsibilities.</p>
3.	Asset Inventory to be maintained
	<p>The Application Administrator should maintain an up-to-date Inventory of the Applications giving details as necessary including location, name of the vendor, name of the application custodian, business supported, history of upgrades, details of Annual Maintenance Contract etc.</p>



SN	Procedures
4.	Segregation of the Environments The development and the Test Environment should be segregated from Production and DR environments. It should be ensured that the developers do not have access to the production and DR environment.
5.	Controls over Installation – Installation kit to be secured The Application administrator should ensure that the Installation KIT is secured, recorded and handed over to the designated Application Owner for safe storage and custody. This will help ensure against unlicensed installations of the Application System.
6.	Only the required components to be Installed Only those components which are necessary for the business should be installed. This will help ensure that the system is not supporting unnecessary services and that associated vulnerabilities are eliminated.
7.	Controls over the Integrity of the System Systemic controls should be implemented to check the integrity of the core system. E.g. the administrator / Application Service Provider should consider implementing the hashing/checksum controls to check the Integrity of the systems at regular intervals.
8.	Input – Processing and Output Controls Various Input controls should be defined, designed, developed, implemented and tested during the User Acceptance Testing as under Input Controls Application Input Controls Various Input controls like Edit Checks, Range Checks, Existence Checks, Field Checks, etc. should be defined and implemented by the Application Vendor or development team. Processing Controls During the processing of various inputs, the Application should be designed to exercise adequate controls. E.g.



SN	Procedures
	<ol style="list-style-type: none">When the user password is HASHED / ENCRYPTED, the password should not be visible / intercept-able to any user including the Administrator in any manner including from processes and memory dumps of the Operating System.Any file uploaded by any user should be stored in a manner which is not accessible to any user including even to the OS Administrator.Logs for financial and non-financial transactions should be generated and stored securely for all activities done by ALL Users including the Administrator and privileged user IDs.
	Output Controls
	<p>The outputs could be printouts or intermediate data files to be used in the next chain of processes in which case appropriate checks should be implemented to ensure the integrity of these intermediate files.</p> <p>Appropriate controls should be implemented to ensure that these outputs are not abused OR cannot be accessed by unauthorized users</p>
9.	Controls over Interfaces and Intermediate Files
	<p>The Interfaces/upload facilities / intermediate files used in the Application should be controlled for type of file, size of the file, integrity checking, and the confidentiality of the contents and secured against unauthorized modification and copying.</p>
10.	Maker – Checker Controls over Inputs
	<p>Maker - checker control should be implemented over the critical activities done by the Application Administrators e.g. creation, modification, and deletion of the user IDs in the Application, changes to the parameter files, defining new products, etc.</p> <p>Similarly, maker – checker controls should also be implemented over the transactions done by general users of the application.</p> <p>As a principle, one user should not be able to complete a transaction end-to-end.</p>



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेट शेड्युलड बँक)

SN	Procedures
11.	User Acceptance testing
	The Application should be tested and signed off for business functionality and security controls before it is moved into the production environment.
12.	Controls over scripts developed outside of the Application
	Any scripts which are developed outside of the Application for additional functionality should be tested, and documented and integrity control maintained. Further access to these scripts should be controlled on the Operating Systems and/or databases.
13.	User Access Management Controls
	Please refer to the “User Access Management Procedures”
14.	Password Controls
	Please refer to the “Password Management Procedures”
15.	Log Management Controls
	Please refer to the “Log Management Procedures”
16.	Change Management Controls
	Please refer to the “Change Management Procedures”
17.	Security Incident Management Controls
	Please refer to the “Security Incident Management Procedures”
18.	Data Backup, Recovery and Retention Policy
	Please refer to the “Data Backup, Recovery and Retention Policy”

Responsibilities

The Bank has moved the Application and supporting infrastructure including the hardware to ESDS-Nashik. The Bank is responsible for the administration of the CBS Application and MPLS Branch Network. The other supporting infrastructure like the Database, Operating Systems and Network devices are administered by ESDS-Nashik.

- The Bank is responsible for CBS Administration



3.2 Database Security Policy

Objectives

- To define appropriate controls to ensure that databases in The Bank environment are adequately secured, logged and monitored.
- Database systems are kept with the latest patches and upgrades
- An appropriate backup strategy is defined to ensure business continuity.

Scope

This policy is applicable to all databases used in The Bank environment and is applicable to all users including employees, contractors, consultants and temporary users.

The Bank has moved the Application and supporting infrastructure including the hardware to ESDS-Nashik. The Bank is responsible for the administration of the CBS Application and MPLS Branch Network. The other supporting infrastructure like the Database, Operating Systems and Network devices are administered by ESDS-Nashik.

Policy Statement(s)

1. Ownership shall be established for each database
2. Procedures shall be established for the installation and upgrade of databases
3. Access to the database shall be controlled
4. Databases shall be monitored regularly
5. Transaction logs shall be monitored regularly
6. Critical databases shall be mirrored on separate disks
7. Procedures shall be established for the backup/recovery of databases
8. Procedures shall be established for the security of databases
9. Procedures shall be established for User Access Management Controls
10. Procedures shall be established for Password Management Controls
11. Procedures shall be established for Log Management Controls
12. Procedures shall be established for Change Management Controls
13. Procedures shall be established for Security Incident Management Controls
14. Procedures shall be established for Data Backup, Recovery and Retention Policy Controls

Procedures

SN	Procedures
1.	Database Ownership and custodian
	<ul style="list-style-type: none">• The Business Owner shall be responsible for the confidentiality, integrity and availability of the Database.



SN	Procedures
	<ul style="list-style-type: none">The Database In-Charge/IT Manager /DBA will be the custodian of the databases.
2.	Database installation and Upgrade
	<p>Manager - IT Service shall:</p> <ul style="list-style-type: none">Review the security features of the Database before installationIdentify, document and test the security features of the Database before installation to the production sites.Monitor for the latest upgrades available for any Database used within The Bank and released by the vendor. These upgrades shall be tested to evaluate the impact on the security of the Database before installation to the production sitesDocument and implement the security controls specific to each databaseThe database should be installed in a separate folder other than the program files.
3.	Control over access to Database
	<ul style="list-style-type: none">OS-level file and directory permissions should be strictly restricted and access should be given “On Need” basis. Ideal permissions for data, logs and control directories are given below for reference<ul style="list-style-type: none">➤ Read-Write to only the Owner➤ Read to Group (Database Administration Group)➤ None to OthersAccess to the database and related files for users should be restricted through the application only.Password changes for default users should be enforced.Users should be created “On Need” basis only with strictly restricted permissions, and “granting” of further rights should be avoided.
4.	Databases must be monitored regularly
	<p>Free space in the databases should be regularly monitored and new space be added after considering the requirements in consultation with the application owner/s.</p>



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेड्युलड बँक)

SN	Procedures
5.	Transaction logs monitoring Transaction logs disk space should be continuously monitored.
6.	Critical database mirroring Critical databases should be mirrored on separate disks for recovery from system, file, or component failure.
7.	Backup / Recovery procedures Properly documented backup/recovery procedures should be in place. This documentation should contain information about the type of backup, periodicity, location, restoration, testing and other relevant details.
8.	Security of database <ul style="list-style-type: none">• An up-to-date record should be kept for the security patches for databases to ensure that the latest security patches are applied immediately. Normally, the application of patches should be done taking a scheduled downtime. However, if there is a need to apply emergency patches, such updates should be made even as an unscheduled activity with the approval of the Business / Application Owner.• To ensure the integrity of the production database, there should be a clear-cut bifurcation between the production and development database environments.• To ensure confidentiality, production data should NOT be populated into the development environment unless authorized. Even after authorization, all production data should be thoroughly “sanitized” before it is populated in the development environment.• Access to data stored on tape backups, data mirrors or any derived exported data should be restricted by using appropriate security controls.• A detailed hardening document should be prepared for each type of database platform. All databases created for / being moved to the production environment should be subjected to the hardening process as specified in this document.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेट शेड्युलड बँक)

SN	Procedures
9.	User Access Management Controls
	Please refer to the “User Access Management Procedures”
10.	Password Controls
	Please refer to the “Password Management Procedures”
11.	Log Management Controls
	Please refer to the “Log Management Procedures”
12.	Change Management Controls
	Please refer to the “Change Management Procedures”
13.	Security Incident Management Controls
	Please refer to the “Security Incident Management Procedures”
14.	Data Backup, Recovery and Retention Policy Controls
	Please refer to the “Data Backup, Recovery and Retention Policy”

Responsibilities

The Bank has moved the Application and supporting infrastructure including the hardware to ESDS-Nashik. The Bank is responsible for the administration of the CBS Application and MPLS Branch Network. The other supporting infrastructure like the Database, Operating Systems and Network devices are administered by ESDS-Nashik

- The CBS Database administration is performed by ESDS

॥ सहकारेण जनकल्याणम् ॥



3.3 Operating System Security Policy

Objectives

Establish adequate controls for the security of the operating systems in The Bank environment and ensure that they are duly protected against misuse and/or unauthorized access. This Policy is designed to ensure that

- The integrity of the Operating System is ensured.
- Access to the files, folders and other system utilities is controlled.
- Access to the operating system is controlled, logged, monitored and analysed.
- The Operating System is adequately protected against the threats of viruses and malware

Scope

This policy is applicable to all server and desktop Operating Systems installed within The Bank environment and is applicable to all users including employees, contractors, consultants and temporary users.

Policy Statement(s)

1. Minimum Baseline Security Controls (OS hardening) for all Operating Systems shall be defined, implemented and recorded
2. Physical and environmental controls over hardware
3. Procedures shall be established for logical access security
4. Each user shall be assigned a separate personal / home directory
5. Procedures shall be established for file system design
6. Procedures for reporting information security incidents on the operating systems shall be established
7. An appropriate login process to Operating System shall be established
8. Correct setting of computer clocks shall be ensured
9. Procedures shall be established for ensuring software installation restrictions
10. Monitoring procedures shall be established
11. Capacity planning procedures shall be established
12. Procedures shall be established for hardware, warranties and replacement
13. Procedures shall be established for Virus Protection
14. Procedures shall be established for User Access Management Controls
15. Procedures shall be established for Password Management Controls
16. Procedures shall be established for Log Management Controls
17. Procedures shall be established for Change Management Controls
18. Procedures shall be established for Security Incident Management Controls
19. Procedures shall be established for Data Backup, Recovery and Retention Policy Controls



Procedures

SN	Procedures
1.	Operating Systems security
	Minimum Baseline Security Controls (OS hardening) for all Operating Systems should be defined and maintained. All installations of the operating systems should be configured as per this baseline security standard.
2.	Physical and Environmental controls over hardware
	<ul style="list-style-type: none">• All servers shall be hosted at the Data Centre - ESDS Nashik OR at the Server Room in the DR location at ESDS Mumbai.• Access shall be limited to members of the IT Team.• All servers shall be marked/tagged as per the naming convention defined by AUCB.• All servers shall be protected from surges, spikes, and sags in the electricity supply by the use of stabilizers and Uninterruptible Power Supplies.• All servers shall be protected from excessively high or low temperatures by temperature control.• All servers shall be protected from excessively high or low humidity by humidity control.• All servers shall be situated in racks, raising them above ground level and therefore reducing the liability of damage through flooding.• All environmental control equipment shall be regularly maintained.
3.	Logical Access Security
	<ul style="list-style-type: none">• Access to server operating systems shall only be granted to the System Administrators in the IT team.• Unused services and applications shall be disabled where practical.• Wherever necessary static IP Addresses may be considered for servers.• Access to services shall be logged and/or protected through access-control methods, if possible.• Remote access to server operating systems shall only be granted to System Administrators on authorization by IT Manager on a need basis only.



SN	Procedures
	<ul style="list-style-type: none">• User access, where facilitated, shall be provided on a basis of least privilege, tight Group Policy implementation, granular access controls and limited access to programs.• Use of utility programs shall be restricted to members of the System Administration Team.• Desktop sessions on a server shall automatically lock after being inactive for 5 minutes. Desktop server sessions will only be available by encrypted Remote Desktop Protocol connections.• As large processing jobs need to be undertaken within sessions, inactive sessions shall not shut down, nor shall a restriction on connection times be imposed. The only method a session shall be reconnected is by the re-authentication of the appropriate user account.• Server software and firmware shall be patched in a timely manner. The most recent security patches shall be installed on the system at the time of installation, except if the immediate application interferes with business requirements. Noncritical and test servers shall be patched first to test the system and application operability.• Policy implementation shall be periodically reviewed every after one month and shall reflect in House Keeping Reports for Servers.• Access to OS files/directories, OS commands and sensitive utilities must be restricted to only those individuals who require them to perform their job functions.• Access to start-up and configuration files must be restricted to the System Administrator only, to prevent unauthorized modification of these files. All unnecessary services must be commented out of the configuration files to prevent unauthorized use of these services.• Wherever applicable, access to various system utilities must be controlled to ensure that the Users do not obtain more information than what they require to perform their job function.• Access to backup utilities must be restricted to only those individuals who require executing them.



SN	Procedures
4.	Home Directories
	Each user must be assigned a separate personal / home directory. A user must not have access to another user's home directory.
5.	File System design
	<p>The System Administrator must design the file system keeping the following points in mind:</p> <ul style="list-style-type: none">• Operating system program files, live application program files, device files or hidden directories with program files in them must not be present in a user's home directory. These must be installed in a separate file system.• Live or production data must be kept in a separate file system• Test / Demo applications must be installed and tested on a separate server. Wherever a test/demo server cannot be provided, a separate file system must be created for the test/demo applications.• The Systems Administrator must keep a record of the entire above-designed file systems.
6.	Reporting of suspicions
	Whenever a system has been suspected of being compromised, it should be immediately reported to the Manager of IT and the respective Group Head. Similarly, all recent changes to user and system privileges must be reviewed for unauthorized modifications.
7.	Login Setting
	<p>The login process to Operating System must</p> <ul style="list-style-type: none">• Not display system or application identifiers until the login process has been successfully completed.• Display a legal caption, warning the Users that the computer must only be accessed by authorized Users• Not provide help messages during the login procedure that would aid an unauthorized User.



SN	Procedures
	<ul style="list-style-type: none">Validate the login information only on completion of all input data. If an error condition arises, the system must not indicate which part of the data is correct or incorrect.Date and time of the previous successful login and details of any unsuccessful login attempts since the last successful login shall be displayed on completion of a successful login where feasible.
8.	Clock Setting
	<p>The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard, e.g. Universal Coordinated Time (UCT) or local Indian standard time (IST). As some clocks are known to drift with time, there should be a procedure that checks for and corrects any significant variation.</p> <p>Use network time protocols: Consider using network time protocols (NTP) to keep your clock synchronized with a trusted time source,</p>
9.	Software Installation Restrictions
	<ul style="list-style-type: none">All software on servers shall be authorized and requested by system owners and shall only be installed by the Systems Administrator.All software installations, updates and removal shall be subject to the Change Management Policy.Regular reviews of software and data content on servers classed as mission-critical must be carried out and reviewed by IT Manager.Unauthorized software or data shall be removed.
10.	Monitoring Procedures
	<ul style="list-style-type: none">Server status and Operating System performance, including system resource usage (CPU, Memory and Disk Logs) shall be monitored.



SN	Procedures
	<ul style="list-style-type: none">Audit logs shall record user activities, exceptions and information security events. System administrator and system operator activities shall also be logged.All security-related events on critical or sensitive systems shall be logged and audit trails saved for a minimum preceding 30 days.Security-related events will be reviewed by the IT team and report critical incidents by the IS Committee. Corrective measures shall be prescribed as necessary.
11.	Capacity Planning
	<ul style="list-style-type: none">The Administration and/or IT Department is responsible for calculating the capacity requirements for serversWhile calculating the capacity of any server, the IT Manager should work closely with the Business Heads to understand the present and projected volumes for a reasonable period in future.It is necessary that the installed capacity should be continuously monitored by the IT Department, to ensure that it is adequate and meets the user and business requirements. Threshold limits should be established for servers and utilisation should be monitored against these threshold limits. Wherever necessary, automated warning signals should be sent out to the designated users whenever the utilisation exceeds the threshold limits.
12.	Hardware Warranties and Replacement
	<ul style="list-style-type: none">Minimum Server Hardware Redundancy such as Power Supply, Hard Drives, NIC, etc. shall be maintained.All production servers shall be under warranty or AMC.When servers are removed from service, their hard drives shall be removed and degaussed before disposal.
13.	Virus Protection
	Please refer to the "Virus Protection Procedures"
14.	User Access Management Controls
	Please refer to the "User Access Management Procedures"



SN	Procedures
15.	Password Controls
	Please refer to the "Password Management Procedures"
16.	Log Management Controls
	Please refer to the "Log Management Procedures"
17.	Change Management Controls
	Please refer to the "Change Management Procedures"
18.	Security Incident Management Controls
	Please refer to the "Security Incident Management Procedures"
19.	Data Backup, Recovery and Retention Policy Controls
	Please refer to the "Data Backup, Recovery and Retention Policy"

Responsibilities

The Bank has moved the Application and supporting infrastructure including the hardware to ESDS-Nashik. The Bank is responsible for the administration of the CBS Application and MPLS Branch Network. The other supporting infrastructure like the Database, Operating Systems and Network devices are administered by ESDS-Nashik.

- The CBS Operating System administration is performed by ESDS

॥ सहकारेण जनकल्याणम् ॥



3.4 Network Security Policy

Objectives

The Bank has engaged ESDS to manage its' Information Technology Infrastructure including the Network devices. The Bank has subscribed to the BSNL MPLS network for connecting the branches to the ESDS network and performing banking operations. ESDS is managing not only The Bank's IT Infrastructure at its data centre but also managing the MPLS network. ESDS is also responsible for defining and implementing security controls over the Network devices.

The main objective of the Network Security Policy is that The Bank's Network should be appropriately secured, redundancies maintained for availability and monitored. Further, ESDS should ensure that the impact of network events on other shared network clients is minimal on The Bank's performance.

Scope

This policy is applicable to all Network Devices like data cables, Switches, Routers, Firewalls etc. including those devices managed by ESDS and not managed by ESDS. This policy is applicable to all users including employees, contractors, consultants and temporary users.

Policy Statement(s)

1. Ownership of network assets shall be established
2. Up-to-date network diagrams shall be maintained
3. Ensure that the network devices are tested before moving into the production environment
4. Segregation in networks at ESDS
5. Adequate redundancy shall be built into the network design
6. Default passwords of all network equipment shall be changed
7. Record of Firewall Policy and Rule Base
8. Firewall logs/audit trails should be enabled
9. Review of firewall logs and audit trails.
10. Procedures shall be established for firewall alerts
11. Procedures shall be established for firewall backup and availability
12. The record should be maintained for firewall operations
13. Procedures shall be established for network monitoring
14. Procedures shall be established for User Access Management Controls
15. Procedures shall be established for Password Management Controls
16. Procedures shall be established for Log Management Controls
17. Procedures shall be established for Change Management Controls
18. Procedures shall be established for Security Incident Management Controls
19. Procedures shall be established for Data Backup and Recovery Controls



Procedures

SN	Procedures
1.	Assigning Ownership
	All Network Devices whether managed by ESDS or not will be the ownership of The Bank unless those are owned by other entities.
2.	Network Diagram
	<ul style="list-style-type: none">ESDS should prepare and maintain a Network Diagram. ESDS should provide the diagram to The Bank.ESDS should review the network diagram to ensure that the diagram is updated to reflect the current network architecture.
3.	Adequate Testing
	ESDS should ensure that any new Network device is adequately tested before moving into the production environment. The test report should be held on record and also provided to The Bank.
4.	Segregation in networks at ESDS
	<p>The Bank understands that the ESDS network is shared between several other clients of ESDS.</p> <p>However, ESDS should ensure that the impact of any event in another client network does not affect The Bank's network performance.</p>
5.	Redundancy to be built into the Network design
	To ensure business continuity (availability of Network), ESDS should build and implement adequate redundancy into the Network design.
6.	Default Passwords to be changed
	<p>ESDS should ensure that the default passwords of all network equipment (e.g. routers, switches) are changed immediately after installation. Similarly, the default community strings must be changed to something which is not guessable.</p> <p>ESDS should implement good password procedures.</p>



SN	Procedures
7.	Record of Firewall Policy and Rule Base
	ESDS should ensure that a record of the Firewall Rules is kept for verification. Every change done in the Firewall rules should be informed to The Bank.
8.	Firewall Audit Trail
	ESDS should ensure that the firewall logging capability is enabled. The Firewall shall be configured to ensure that all network transactions are logged and the time stamps, source, destination host and ports used are recorded. ESDS should maintain a Firewall audit trail and should provide it for verification or monitoring whenever required by The Bank.
9.	Review of Firewall Logs and Audit Trails
	ESDS shall ensure that access to logs and audit trails is restricted to authorized users only. All firewall logs and audit trails will be considered highly confidential information. ESDS should cooperate and show the record/audit trails of Firewall policy and rules to The Bank OR its' representation OR The Bank nominated system auditor.
10.	Firewall Alerts
	ESDS should ensure that the firewalls are configured to generate real-time alerts and notifications to the designated users. In case of any malicious activity noticed on the firewall, ESDS should immediately inform The Bank about such events and the steps taken to mitigate the risks.
11.	Firewall availability and Backup Procedures
	ESDS should ensure that high availability is maintained by implementing redundant and load-balancing firewalls. Further the Firewall configuration, logs and audit trails are backed as required.
12.	Record of firewall operations
	ESDS should maintain the following documentation <ul style="list-style-type: none">• Approved Firewall configuration and rule-based documentation• Firewall Configuration Review Reports• Approved Network (Firewall) Change Management Forms• Firewall Monitoring Reports



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेट शेड्युलड बँक)

SN	Procedures
	<ul style="list-style-type: none">• Root cause analysis reports. Reviewed and approved a list of personnel with access to the firewall along with their levels of access.
13.	Network monitoring
	ESDS should ensure that the network devices are monitored as per the SLA and ensure compliance with the RBI Guidelines and best practices
14.	User Access Management Controls
	Please refer to the "User Access Management Procedures"
15.	Password Controls
	Please refer to the "Password Management Procedures"
16.	Log Management Controls
	Please refer to the "Log Management Procedures"
17.	Change Management Controls
	Please refer to the "Change Management Procedures"
18.	Security Incident Management Controls
	Please refer to the "Security Incident Management Procedures"
19.	Data Backup, Recovery and Retention Controls
	Please refer to the "Data Backup, Recovery and Retention Policy"

Responsibilities

The Bank has moved the Application and supporting infrastructure including the hardware to ESDS-Nashik. The Bank is responsible for the administration of the CBS Application and MPLS Branch Network. The other supporting infrastructure like the Database, Operating Systems and Network devices are administered by ESDS-Nashik.

- The Network administration, monitoring, incident management and ensuring availability are performed by ESDS



3.5 E-Mail Security Policy

Objectives

- Ensure that the e-mail facility provided to the users is used for authorized purposes only.
- Protect the Information Assets from various threats related to the usage of E-mails like viruses, spam mail, leakage of information through e-mails etc.
- E-Mail usage should be logged and monitored.
- To encourage an efficient communication system to add value to the services offered by The Bank.
- Implement adequate usage controls to ensure that the email facility provided by The Bank is used only for official purposes. e.g. content filtering, mail box size restrictions, mass mailing controls, attachment size controls etc.
- Implement adequate security controls to ensure that the vulnerabilities associated with email facilities are minimized e.g. antivirus etc.
- Educate the users about the applicability of this policy.

Scope

This policy is applicable to the infrastructure supporting the E-mail services like E-Mail Server, Mail Box server, E-Mail application, etc. and is applicable to all users including employees, contractors, consultants and temporary users.

Policy Statement(s)

1. Procedures shall be established for controlling e-mail access
2. Users shall access only the approved client email software
3. Users shall not abuse e-mail access
4. Procedures shall be established for restricting access to other user's e-mail account
5. Users shall not open e-mails/attachments received from an unknown source
6. All incoming and outgoing mails shall be scanned for viruses and content filtering
7. The Bank can inspect the email and attachment contents of any user at any time without notice
8. Auto forwarding of e-mails shall be restricted
9. Sending of critical information through e-mails shall be controlled
10. The attachment size of e-mails shall be restricted
11. Every e-mail shall contain a standard and approved disclaimer
12. Every user shall adopt a standard e-mail signature approved by The Bank
13. Procedures shall be established for ensuring proper backups of e-mail files
14. Access to Emails from outside of The Bank's Network shall be controlled
15. Controls over distribution email Ids shall be established
16. Procedures shall be established for securing and maintaining e-mail logs
17. Procedures shall be established for User Access Management Controls
18. Procedures shall be established for Password Management Controls



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेट श्रेष्ठबुलड बँक)

19. Procedures shall be established for Log Management Controls
20. Procedures shall be established for Security Incident Management Controls

Procedures

SN	Procedures
1.	Controls over E-Mail Access
	Access to the e-mail facility from The Bank infrastructure should be given to only those users who have a business need and are approved by the Asset Custodian.
2.	Only tested and approved e-mail Software
	The users should be allowed to access their emails using The Bank Approved client email software only.
3.	User Responsibility
	<ul style="list-style-type: none">Each user will be held accountable for the contents of his / her email. Each user must have a distinct and unique e-mail ID to help establish accountability.The usage of the e-mail facility shall be primarily for business purposes.In case of any unusual activity like chain mail, spam emails, virus emails, etc. the user should report it to the Departmental Head.
4.	Restriction on the use of another user's email ID
	<p>Users accessing the e-mail services of The Bank must not use or access an e-mail account assigned to another individual to either send or receive messages.</p> <p>If there is a need to read other users' e-mail (while he /she are away on vacation for instance), then message forwarding and other facilities should be used instead. Approval from the Department Head must be obtained in case a user's e-mail needs to be read in his / her absence.</p> <p>At times emails of some persons need to be accessed on an ongoing basis by other/s (E.g. Secretary accessing the Boss's email or a Project email id accessed by team members), such facility should be used/allowed only for receiving or reading emails and not for sending mails through that ID. i.e. such shared and generic IDs must be used for only receiving emails but not for sending mail. Further, such a facility should be allowed only after formal approval from the business head or from the person whose ID is being used.</p>
5.	Mails from Unknown Sources
	Opening e-mails and attachments from unknown or untrusted sources is STRICTLY PROHIBITED.



SN	Procedures
6.	Virus and other controls
	All incoming and outgoing mail should be subjected to scanning for viruses.
7.	Right to review e-mail contents
	The E-mail facility used by the Infrastructure of The Bank is the property of The Bank. Accordingly, The Bank can inspect the email and attachment contents at any time and without notice,
8.	Restrictions on Auto Forwarding of emails
	No email, automatic or otherwise, shall be forwarded to personal or another user official and public email account unless required by business
9.	Controls over sending critical information through emails
	Highly critical and confidential information like passwords, etc should not be sent through a normal email facility (not encrypted). Any other confidential documents sent by email should be password protected and the password should be communicated to the recipient in a secure manner.
10.	Attachment Size Restrictions
	The maximum attachment size should be restricted to 25 MB only. If any user needs an increased attachment size, an appropriate exception should be obtained.
11.	Standard Disclaimer for all emails
	A standard disclaimer would be appended to every email sent outside of The Bank Network.
12.	E-mail Signature
	A standard email signature format will be provided by The Bank and every user should follow the format.
13.	Backup of Emails
	<p>The IT Department should ensure that adequate backups of emails on the server are taken</p> <p>In case of a user needs to backup his emails for valid business reasons, the IT department should organise the backup, after obtaining appropriate approval from the requestor's manager.</p>



SN	Procedures
14.	Access to Emails from outside of The Bank's Network
	Access to Emails from outside of The Bank's Network should be granted only against appropriate approvals from the user's manager.
15.	Controls over distribution email Ids
	Distribution email IDs help in sending mass emails to a section or the whole of The Bank. However, such distribution IDs may be abused and hence access to such distribution IDs should be controlled as under <ul style="list-style-type: none">• Mails to such IDs should be allowed to the identified user IDs only• Mailing to such IDs should be allowed only from the corporate network• Any emails received from outside of the corporate domain should be kept in a separate folder for further investigation. The mail should not be forwarded to the member's email IDs.
16.	E-mail Logs
	Logs for emails should be secured and maintained for the period defined by The Bank.
17.	User Access Management Controls
	Please refer to the "User Access Management Procedures"
18.	Password Controls
	Please refer to the "Password Management Procedures"
19.	Log Management Controls
	Please refer to the "Log Management Procedures"
20.	Security Incident Management Controls
	Please refer to the "Security Incident Management Procedures"

Responsibilities

- Manager-IT
- E-mail administrators
- The users to whom e-mail access is granted



3.6 Internet Security Policy

Objectives

- To establish adequate security controls over the access/usage of the internet through The Bank network.
- Ensure that only authorised users are allowed access to the Internet.
- Ensure against malicious codes like viruses and worms
- To log and monitor the access to the internet.

Scope

This policy is applicable to all the infrastructure assets which are used for internet access like Proxy, Content Filtering Software, Network components etc. and is applicable to all users including employees, contractors, consultants and temporary users.

Policy Statement(s)

1. Access to the internet shall be provided for business purposes only
2. Procedures shall be established for control over internet access
3. All the material downloaded from the internet shall be screened by updated anti-virus
4. Procedures shall be established for internet log monitoring
5. Procedures shall be established for restricting abuse of internet access by users
6. Procedures shall be established for User Access Management Controls
7. Procedures shall be established for Log Management Controls
8. Procedures shall be established for Security Incident Management Controls

Procedures

SN	Procedures
1.	Access to Internet
	<p>Access to the Internet must be provided only to those employees who have a legitimate business need for such access. The authorization to access the Internet for an individual depends on:</p> <ul style="list-style-type: none">• The nature of work requires the User to connect to the Internet.• The sites that he/she is authorized to access the Internet.



SN	Procedures
2.	Control over Internet Access
	<ul style="list-style-type: none">• All Internet activity must pass through Bank's & ESDS Firewall so that access controls and related security mechanisms can be applied.• Internet access shall be restricted to authorized individuals only.• Internet usage, if any, should be restricted to identified standalone computer(s) in the branch of a Bank which is strictly separate from the systems identified for running day-to-day business. If allowed in any of such endpoints, the same should be adequately secured through proxy servers on an ongoing basis• Sites that are not related to the business activities of The Bank shall be restricted during normal working hours.• Sites providing offensive/indecent content shall be blocked at all times.• Downloading of files like *.exe, *.mp3, *.mpg, etc. shall be restricted.• All Internet services and applications (like instant messengers, file-sharing applications, Social Networking Sites, etc.) which are not required for a business need must be disabled or uninstalled. If such applications are required, they should be installed after authorization by the Manager of IT.
3.	Downloads
	All information downloaded e.g., Email retrieval, data / FTP downloads, Active x controls, Java, Java Applets, images etc., to The Bank computing resources via the Internet must be screened with updated virus detection software prior to use.
4.	Log Monitoring
	Routine logs of websites visited, files downloaded, and related information must be maintained and reviewed regularly by the Internet system administrator. He must report unusual activities to Manager IT.
5.	Restrictions on Users
	<ul style="list-style-type: none">• Users are not allowed to host personal sites using The Bank facilities• Users using The Bank computers on discovering that they have connected with a website that contains potentially offensive material must immediately disconnect from that site.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड श्रेड्युलड बँक)

SN	Procedures
	<ul style="list-style-type: none">The ability to connect with a specific web site does not in itself imply that users of The Bank systems are permitted to visit that site.The use or attempt to initiate such activities using The Bank computing facilities or equipment leading to abusive, unethical or “inappropriate” use of the Internet is considered grounds for disciplinary, legal and/or punitive actions, including termination of employment.At any time and without prior notice, The Bank management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, and other information stored on or passing through The Bank computers.Users must not place The Bank information or material (confidential information, internal memos, etc.) on any publicly accessible Internet computer, which supports anonymous FTP or similar services unless the Group heads and IT Manager have first approved the posting of such materials.
6.	User Access Management Controls
	Please refer to the “User Management Procedures”
7.	Log Management Controls
	Please refer to the “Log Management Procedures”
8.	Security Incident Management Controls
	Please refer to the “Security Incident Management Procedures”

Responsibilities

- Manager-IT
- Network Administrator
- The users to whom internet access is granted



3.7 Desktop and Laptop Security Policy

Objectives

- To ensure adequate control over the usage of The Bank's desktops and laptops.
- To protect The Bank's information systems and assets through appropriate controls over the usage of external media and software applications.
- To ensure that the end-user who has been allotted a desktop/laptop is made aware of his / her responsibility towards The Bank's asset.
- To reduce the risk of theft of assets/data by maintaining a secure environment.

Scope

This policy is applicable to all geographical units of The Bank and to all the employees, contractors, consultants, partners and third parties.

Policy Statement(s)

1. High-level guidelines for desktop/laptop security shall be established
2. User-level access rights shall be defined
3. Procedures shall be established for ensuring operating systems-level security
4. Desktops / Laptops issued to staff or consultants remain the property of The Bank
5. Procedures shall be established for ensuring the security of desktops/laptops
6. Installation of software on desktops/laptops shall be controlled
7. Users shall return the desktop/laptop while leaving the employment of The Bank

Procedures

SN	Procedures
1.	High-Level Guidelines for Desktop / Laptop Security The high-level guidelines for implementing desktop security are as follows: <ul style="list-style-type: none">• Entry Criteria: Desktop Allocation and Installation• Exit Criteria: Desktop Release and Format• Physical Access Restrictions: Users shall not be allowed to open or move computer systems for any reason• BIOS Settings:<ul style="list-style-type: none">➤ BIOS Setup Password shall be enforced on all the critical desktops and shall be known only to IT personnel.➤ Power-ON/Boot Password shall be enforced on all critical desktops, which will serve as a first level of access security.➤ Booting from active devices like CD-ROM, Floppy Drives, Boot ROM etc... shall be disabled.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेट शेड्युलड बँक)

SN	Procedures
2.	User Level Access Rights
	<ul style="list-style-type: none">• Users shall not be part of administrators or power user groups.• Users shall not be permitted to share any folder on their desktops.• Users shall be advised not to download shareware/freeware software tools from the Internet.• Users shall not be allowed to change basic settings like default IP address, Service packs, System partition and default services etc...• Standard wallpaper and screen saver shall be enabled with password protection with an idle time-out of 5 minutes interval
3.	Operating System Level Security
	<ul style="list-style-type: none">• The issue of the anonymous user account shall be restricted.• Users with valid User IDs and Passwords shall be allowed to log on to the desktop.• Automatic log-on shall be disabled.• Only administrators shall be allowed to change /configure base objects such as files/printers/processes etc...• Page file shall be cleared on system shutdown.• Remote Desktop Protocol (RDP) access services shall be restricted / disabled.• Unauthorised remote access tools shall not be installed on the desktops.• Remote access to the registry shall be restricted to administrators only.• Antivirus software shall be installed on all desktops by default and shall be updated automatically on a regular basis.• For laptops taken out of bank premises, users shall be required to check and update the antivirus signature from a central location. It is advised to users to check for updates on a daily basis for signature updates.• Internet Browser security customization package shall be only for the current logged-in and administrators shall be allowed to shut down the desktops.• The desktop audit shall be performed at a yearly interval.• IT Manager shall review all such reports on a regular basis for compliance checking.
4.	Ownership of Desktop / Laptop
	<p>Desktops / Laptops issued to staff or consultants remain the property of The Bank. When the desktop/laptop is allocated to the individual, the user officially assumes "temporary custodianship" of the desktop/laptop.</p>



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेड्युलड बँक)

SN	Procedures
5.	Security of Desktop / Laptop
	<ol style="list-style-type: none">1. All the users must agree to take FULL responsibility for the security of their desktop/laptop and the information it contains.2. Upon allocation of the laptop, the user must complete and sign a "Laptop Declaration form".
6.	Software on Desktop / Laptop
	<ol style="list-style-type: none">1. Users must take all reasonable steps to protect against the installation of unlicensed or unauthorized software and malicious software.2. The use of unlicensed software (software piracy) is illegal and puts The Bank at significant risk of legal action.3. Executable software must, whenever possible, be validated and approved by their Manager before being installed into the IT environment.4. Unmanaged installations can compromise the IT operating environment and also constitute a security risk, including the intentional or unintentional spreading of software viruses and other malicious software.5. Commercial software (including shareware) must -<ul style="list-style-type: none">➤ Have a valid license for each prospective user➤ Be checked for all known security risks, including malicious software6. Desktop and laptop users must ensure they comply with data copyright requirements.
7.	Surrender of Desktop / Laptop
	Upon leaving the employ of, or separation from The Bank, the user must return the desktop/laptop to their manager or supervisor or local IT Team

Responsibilities

- Manager-IT
- IT Support Team



3.8 User Access Management Policy

Objectives

The objective of this Policy is to ensure that

- User Management is standardized and governance controls are implemented over the Registration, Modification and De-registration of users.
- Access is granted to the users as per business requirements and only against approval from the designated authority.
- Users are informed about their legitimate accesses and also educated about the consequences of access violations.
- Reviews are done of the user management process.

Scope

This policy is applicable to all geographical units of The Bank and to all the employees, contractors, consultants, partners and third parties.

Policy Statement(s)

1. Procedures should be established for control over default users
2. Procedures should be established for user creation, modification and deletion
3. Procedures should be established for the identification of dormant and inactive user ids
4. Procedures should be established for the reissue of a deleted user ID
5. Procedures should be established for assigning roles and groups to users
6. The naming convention should help uniquely identify a user on the system
7. Each user Id should be uniquely identified on a system
8. Procedures should be established for control over generic user ids
9. User ID should be locked after three failed logging attempts
10. Procedures should be established for control over temporary user ids
11. User inactivity time-out should be configured
12. Adequate segregation of duties should be enforced
13. Maker – Checker Controls should be established.
14. Regular review of Users and their Privileges should be carried out



Procedures

SN	Procedures
1.	Controls over Default Users
	Many systems (Applications, Databases, Operating Systems, routers etc.) have default user IDs which are required for Installation/initiation and maintenance. Also, many times the passwords for these IDs are public information (e.g. user IDs and passwords for Oracle, MSSQL etc.).
	As a best practice, these users' IDs should be disabled/deleted OR renamed and the passwords should be changed. This will help ensure that any malicious/unauthorized activity cannot be performed using the default user ID and password.
2.	User Creation, Modification and Deletion
	<ul style="list-style-type: none">• Users of the Information Asset can be of various Types - At the broad level, there would be two types of users - Administrator and General User. For each asset like Operating System, Database, Application, and Network Components, there will be these two types of users.• A process should be defined and implemented to ensure that any new user creation, modification or deletion is for the business purpose, documented, approved and record maintained for future reference.• A User EXIT process should be defined and implemented to ensure that the user ID is disabled/deleted when a user exits from The Bank.• Where necessary the user ID should auto-expire on a predefined date (e.g. in the case of temporary users)• A deleted user ID should not be PURGED but labelled as "deleted".• Further, the system should ensure that a deleted / disabled ID cannot be issued to any other user in The Bank, except as mentioned in the next section.
3.	Identification of Dormant and Inactive User IDs
	Active Directory User IDs which are not active for 30 or more days should be identified, documented and disabled after approval. In case such IDs are to be activated, the procedures mentioned in the next section should be followed. The CBS User IDs which are not active for 7 or more days should be identified, documented and disabled after approval. In case such IDs are to be activated, the procedures mentioned in the next section should be followed.
4.	Reissue of a deleted User ID



	<p>An inactivated user ID may be again activated if necessary, against approvals and must be enabled only for the “original user”.</p> <p>This process should be treated at par with the creation of the new user ID and all the related controls like approval, issue of first password, change of password on first logon, record keeping etc. should be followed.</p> <p>This activity should be logged and monitored.</p>
5.	Assignment of Roles and Groups
	<p>Various Systems (Applications, Databases, Operating Systems, etc.) give the users membership of a group, category and role. This membership gives the user various privileges to perform his job responsibilities.</p> <p>A control process should be defined and implemented when a user is given the membership of the group, category or assigned role.</p> <p>The Process should help ensure that the group/role assigned to any user is for business purposes, documented, approved and record maintained for future reference.</p>
6.	Naming Convention
	<p>For all users on other systems (Database, Operating Systems etc.), a naming convention should be defined.</p> <p>The naming convention should help uniquely identify a user on the system.</p>
7.	Unique Identification of each user on a system
	<p>Each user Id must be uniquely identified on a system. One user ID should not be issued to multiple users to ensure that accountability is established.</p>
8.	Generic User Ids
	<p>As a prudent practice creation of generic user Ids should be avoided.</p> <p>However, there are situations where creating unique user IDs itself may result in vulnerability e.g. creating user IDs with root, administrator, sys, system etc. privileges.</p> <p>In such cases, the Custodian of the Information Asset should approve shared usage of such generic user Ids by the identified team members.</p> <p>The Custodian should set up systemic or compensating controls to ensure that although the user ID is Generic, compensating controls and audit trails are available to accurately identify the user and establish accountability for activities carried out using the shared generic user ID.</p>
9.	Locking of a User after Failed Login Attempts
	<p>After 3-5 bad attempts, the user ID should be locked and should be enabled only after the Application Administrator enables it against approval from the owner.</p>



10. Temporary User IDs	
	If a user ID is created for a temporary period, its' expiry date should be entered during the creation process itself. The system should automatically lock the user Id on the designated date.
11. User Inactivity Time Out	
	<ul style="list-style-type: none">• Inactivity time-out should be configured at min. 3 minutes max. to 15 minutes depending on the applicability.• The user should be required to enter his password to unlock the screen.
12. Segregation of Duties	
	Adequate Segregation of Duties should be enforced for conflicting duties. In cases where conflicting duties are required to be performed by the same user, adequate compensating controls like supervision, logs, dual authorisation etc. should be used.
13. Maker-Checker Controls (Never Alone Principle)	
	<p>A maker-checker control should be implemented over the critical or sensitive activities done by any user e.g. creation, modification, and deletion of the user IDs, changes to the parameter files, defining new products, critical systems initialisation and configuration, PIN generation, creation of cryptographic keys, use of administrative accounts etc.</p> <p>Similarly, maker-checker controls should also be implemented over the transactions done by general users of the application.</p> <p>As a principle, one user should not be able to complete a transaction/activity end-to-end.</p>
14. Review of Users and their Privileges	
	The ISC should ensure that a review of Users and their Privileges is carried out during the Security Audits.

Responsibilities

- The Administrators of various systems like Applications, Databases, Operating Systems, Network Components, etc.
- IT Support Team



3.9. Password Management Policy

Objectives

The objective of this policy is to define and implement adequate authentication controls in the form of good password controls and disciplines.

Scope

This policy is applicable to all geographical units of The Bank and to all the employees, contractors, consultants, partners and third parties.

Policy Statement(s)

1. Procedures shall be established for use of a strong encryption algorithm.
2. Default passwords shall be changed before moving the system into the production environment.
3. The System shall enforce a minimum password length.
4. The System shall inform the user that his / her password would be due for a change.
5. The system shall enforce a change of password for a user after it is RESET by the Administrator.
6. The System shall enforce a change of password for a new user at his FIRST login to the system.
7. The System shall enforce a change of password composition.
8. The System shall ensure that new passwords are used for a specified minimum period.
9. The System must enforce the change of password at periodic intervals.
10. The System must enforce the alphanumeric composition of the password.
11. The System must enforce complex composition of passwords.
12. The Users shall not share their passwords with any other user including the administrator.
13. Procedural password controls shall be established.
14. Option for change of password shall be available to the users without the intervention of the Administrator.
15. The system shall not allow the user to select any of his / her past 5 passwords.
16. It must be ensured that the critical passwords are available even when the concerned administrator is on leave or not available.



Procedures

SN	Procedures
1.	Using a strong Encryption Algorithm <ul style="list-style-type: none">The encryption algorithm used for encryption should be strong, tested and proven. The encryption algorithm should not be reversible.The encryption algorithm should produce different encrypted values for the same passwords used by different users.Passwords should be encrypted before being stored in the Application, Database, Operating System, Network Components etc.The File / Table/database in which the passwords are stored should be protected with strong access controls
2.	Default Passwords <ul style="list-style-type: none">Some of the systems are installed with vendor-defined user IDs and passwords. In some cases, these passwords are public knowledge e.g. passwords for sa, sys, system, Scott, etc. At times the vendor would even hard code the password in the application to facilitate maintenance and could be known to several users of the vendor. These passwords are vulnerable.Hence it is necessary that the default passwords are changed before moving the system to the production environment.
3.	Password Length <p>Password is the first and in most cases, the only line of defence and must be enforced in the best possible manner. The System should enforce a minimum 8-character Password.</p>
4.	Notice to the user that the password due for a change <p>The System should inform the user that his password would be due for change by a particular date or after a certain number of days.</p>
5.	Change after RESET <p>The system should enforce a change of password for a user after it is RESET by the Application Administrator.</p>
6.	First login to the system <p>The System should enforce a change of password for a new user at his FIRST login to the system.</p>



SN	Procedures
7.	New Password must be different by a certain number of characters The System should enforce a change of password composition by a minimum of 3 characters i.e. the new password must differ from the old by at least 3 characters. This will ensure that the password change is really effective.
8.	New password to be used for a minimum period The System should be configured to disallow a user to change his / her password for a minimum of 3 days i.e. the user will have to use the new password for a minimum of 3 days before the system will allow him/her to change. This helps ensure that the change of password is effective. In case the user wants to change the password within those minimum mandatory usage days, he/she should approach the administrator with an approved request who will then enable the option to change the password for that user and for that instance only.
9.	Password Aging The password age should be long enough to promote security, but not so short that users become frustrated with constantly having to change their password. A typical password age is between 30-120 days.
10.	Composition of Password - Alpha-Numeric Composition Enforce password complexity rules: When users create a new password, enforce complexity rules such as requiring a minimum length and using a combination of uppercase and lowercase letters, numbers, and special characters.
11.	Composition of Password - Complex Composition <ul style="list-style-type: none">At least for the critical and sensitive logins the System must enforce at least one UPPERCASE, one lowercase and one control character like !, @, \$, ^, etc.The system should not allow a user to use any character more than twice and must enforce that repeated characters are not more than 2 in the password composition.More than 3 successive characters/numbers should not be allowed to be used as a part of the password.
12.	Passwords not to be shared The Users should not share their passwords with any other user including the administrator.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेट शेड्युलड बँक)

SN	Procedures
13.	Procedural Password Controls
	<p>Some of the password-related controls cannot be enforced systemically. These controls must be followed procedurally as under</p> <ul style="list-style-type: none">• Passwords should not be shared• Passwords should not be embedded in scripts and programs because anyone who has access to the source code would be able to know the passwords.• However, there could be circumstances when the passwords are required to be embedded e.g. the backend password used by the application to access the database and should be treated as EXCEPTIONS at the Policy Level itself.• Also, the passwords should not be saved/remembered in the authentication window/prompt, because they can be easily abused.
14.	Password change Option availability
	<p>Option for change of password should be available to the users without the intervention of the Administrator. This will eliminate the dependency of change of password on the administrator.</p>
15.	Passwords History
	<p>To ensure that the change of password is really effective, the system should not allow the user to select any of his / her past minimum of 3 times passwords.</p>
16.	Critical Passwords – To be written on a standard form
	<p>It must be ensured that the critical passwords are available even when the concerned administrator is on leave or not available. This can be ensured by writing down the passwords. (Refer Form Template for Writing the “Passwords for Critical User IDs”).</p>

Responsibilities

- Administrators of various systems – Operating Systems, Applications, Database, Routers, Firewalls etc.
- IT Support Team

xxxxxx End of Policy Documents xxxxxx



4. Information Systems Outsourcing Policy

Objectives

The objective of this policy is to establish procedures for safeguarding The Bank's information system, as well as information from intentional misuse, abuse, damage or disclosure by the third-party resources & suppliers/vendors employed/engaged by The Bank. This policy can also be referred to as 'Vendor Management Policy' or 'Supplier Security Policy'.

Scope

1. Vendor / Third party selection process
2. Vendor / Third Party Obligations shall be documented
3. Vendor / Third parties of The Bank should sign the appropriate Non-Disclosure Agreement
4. Ensure that Vendor / Third Party deploys appropriate personnel
5. Procedures shall be established for training to vendor / third parties
6. Procedures shall be established for incidence response by Vendor / Third Party
7. Procedures pertaining to entry for vendor / third-party resources shall be established
8. Appropriate procedures shall be established for the identification of vendor / Third Party resources by issuing badges, identity cards etc. to them at the entry point.
9. Procedures shall be established for physical access controls for vendor / Third Party Resources
10. Right to audit the vendor set-up

Procedures

SN	Procedures
1.	Vendor / Third-Party Selection Process
	<p>The Bank should define a vendor selection criterion which is based on a comparative analysis of techno-commercial aspects of the proposal/s received from a vendor.</p> <p>Selection of the vendor will be driven by various parameters like technical competency, compatibility with present set-up, support and maintenance, past experience in the vendor in the business line, quality and security certifications by the vendor, DR readiness, financial stability, market reputation, and cost of the product/services.</p>



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपेटिट शेड्युलड बँक)

SN	Procedures
2.	Vendor / Third-Party Obligations
	<ul style="list-style-type: none">The Bank should ensure that the vendor obligations/duties / roles-responsibilities are defined and documented. These obligations/duties/roles and responsibilities should be included in the contract / SLA.The vendor should submit necessary MIS / reports etc. to The Bank to help monitor the performance as per the SLA. ESDS – Nashik has provided one utility “E-Magic” to The Bank to monitor the activities performed by ESDS.In case of any requirements/problems, The Bank should raise a request ticket which will be classified as criticality and accordingly resolved by the vendor / third party.The Service Level Agreement / Contract should clearly specify the Turn-Around-Time for various services for which the vendor is engaged.
3.	Non-Disclosure Clauses
	The Bank should ensure that appropriate clauses are included in the SLA / Contract to ensure that the vendor / third party takes necessary precautions to protect The Bank’s data/information against unauthorised access.
4.	Vendor / Third-Party Personnel
	<ul style="list-style-type: none">The vendor / Third Party should conduct background checks for resources deployed in The Bank engagements.Qualifications, knowledge, experience, etc. of the personnel employed by the vendor / third party should be in line with the job requirements.
5.	Training to Third Parties
	<p>The Bank should include appropriate clauses in the SLA / contract to ensure that the vendor / Third Party trains its’ resources about Information Security requirements.</p> <p>This training should help ensure that the resources understand their obligations, responsibilities and liabilities involved in accessing, processing, communicating and managing The Bank’s data/information and information processing facilities.</p>



SN	Procedures
	This training should be given to each resource and should be repeated at regular intervals.
6.	Incidence response
	The vendor / Third Party Manager should maintain an up-to-date information security incident response plan including mobilization of users in the contact / call trees, bridge numbers, severity assessment, log / record the steps for recovery, evidence collection and process diagrams.
7.	Entry for third-party resources
	<ul style="list-style-type: none">• All third-party resources must sign in at the security point/reception in a Contractors Log that is retained and reviewed by the Administration Manager• All third-party resources must wear a contractor's badge when on the premises of The Bank
8.	Identity Badges
	<ul style="list-style-type: none">• Vendor / Third party resources should wear their identification badges when on Bank's site.• If the resource forgets his identification badge then he must obtain a temporary badge by providing appropriate identification. Such a temporary badge should be valid for a single day only.• Identification badges that have been lost or stolen or are suspected of being lost or stolen must be reported to the Admin Department immediately.
9.	Physical Access Controls
	<ul style="list-style-type: none">• Third-party resources must not attempt to enter into restricted areas in The Bank's premises to which they have not been granted access.• Third-party resources must not permit unknown or unauthorized persons to pass through doors requiring swipe cards/number codes, at the same time when they pass through these entrances.



SN	Procedures
10.	Ensure the Security of The Bank's Information Assets The vendor – in this case, ESDS – Nashik – should ensure that the Information Assets of The Bank under its' custody is adequately secured. Appropriate clauses should be incorporated in the agreement about the implementation of security controls. ESDS should ensure that the information assets which are in its custody are secured as per the RBI guidelines and Bank's Information Security Policies and hardening best practices. ESDS would have shared its' setup with various other organisations. However, ESDS should ensure that The Bank's business is not affected because of incidents/events in the set-up of other organisations. The Bank's set-up should be physically and logically isolated in a separate environment.
11.	Right to Audit the Vendor Set up The Bank should ensure that the appropriate clause for "Right to Audit" is incorporated in the Agreement with the vendor. These audits may include as necessary, a review of vendor security policies and procedures, on-site assessment of physical security arrangements, network, system, and application vulnerability scanning, and penetration testing. Such assessments will be communicated well in advance and conducted at a time mutually agreed upon between the vendor / Third Party and The Bank. The Bank will submit observations raised in these audits to the vendor / Third Party for rectification.

Responsibilities

- IT Infrastructure team
- Administration department

xxxxxxx End of Policy Documents xxxxxxxx



5. Internet Banking Security Policy

Objectives

The objective of this policy is to establish procedures for safeguarding The Bank's Internet Banking infrastructure from various vulnerabilities & risks.

Scope

This policy applies to the proposed Internet Banking Application.

1. Internet Banking Application Vendor Selection
2. Perform functional and Security Testing of the set-up
3. Phased launching of the Internet Banking Application
4. Ensure secure administration of Internet Banking Infrastructure
5. Ensure Logical Access Controls for Internet Banking Infrastructure
6. Ensure Log Monitoring and Intrusion Detection / Prevention
7. Perform periodic vulnerability assessments and penetration tests
8. Ensure adequate Backup Management & Disaster Recovery Controls
9. Procedures shall be established for the Application of Security Controls
10. Procedures shall be established for Database Security Controls
11. Procedures shall be established for Operating System Security Controls
12. Procedures shall be established for User Access Management Controls
13. Procedures shall be established for Password Management Controls
14. Procedures shall be established for Data Backup, Recovery & Retention Controls
15. Procedures shall be established for Change Management Controls
16. Procedures shall be established for Log Management and Monitoring Controls

Procedures

SN	Procedures
1.	Internet Banking Application Vendor Selection
	Please refer to the "Information Systems Outsourcing Policy"
2.	Functional and Security Testing of the set-up
	The Bank should ensure that the Internet Banking Application is tested as under <ul style="list-style-type: none">• Functional Testing is performed in the Test Environment for various types of financial and non-financial transactions as well as security controls• Systems Audit is performed of the Internet Banking Application and associated Web Server, Operating System, Database, Firewall etc.• Vulnerability Assessment and Penetration Testing are performed on the Application as well as on the associated infrastructure



SN	Procedures
	<ul style="list-style-type: none">The development, test and production environments should be segregated.
3.	Phased launching of the Internet Banking Application
	<p>Since Internet Banking is accessible over the Internet by a very large number of customers, The Bank should consider launching the Internet Banking Application in a phased manner under</p> <p>Phase I – After adequate Security Testing, The Bank may consider launching a “View Only” facility through the Internet Banking Application. This facility will restrict the customers to only see their accounts and take a statement of account. They will not be allowed to perform any financial or non-financial transactions.</p> <p>Phase II – After gaining confidence about the success of Phase I, The Bank may consider enabling some types of transactions e.g. allowing customers to register a request for an ATM card, credit card, stop payment instructions, request for a new cheque book etc. The Bank may also consider enabling the creation of FDs by the customer, within Bank transfer of funds, etc.</p> <p>Phase III – After gaining confidence about the success of Phase II, The Bank may consider enabling other features like registering and payment of billers, interbank transactions, etc.</p>
4.	Secure administration of Internet Banking Infrastructure
	<ul style="list-style-type: none">The Bank should define the Standard Operating Procedures for the management and administration of the Internet Banking Application.As a best practice, the administration of Internet Banking Infrastructure should not be performed remotely and over the internet.Segregation between Information Technology & Information Security Department teams should be maintained.As a best practice, the development team/vendor should not be given access to the production environment. However, in case it is necessary to give access to the development team, it should be approved, controlled, logged and monitored.The Bank should designate a Network and Database Administrator with clearly defined roles & responsibilities.The Bank should review its' security infrastructure and security policies regularly and optimize them in light of its own experiences and changing technologies



SN	Procedures
	<ul style="list-style-type: none">Security infrastructure should be tested and user acceptance “signed off” before using the Systems and Applications for internet banking business operations.Bank should periodically upgrade the Systems to the latest versions, which would give better security and control features.The Bank shall obtain an application integrity statement from the vendor/service provider, before implementing the internet banking software.
5.	Logical Access Controls for Internet Banking Infrastructure
	<ul style="list-style-type: none">The Bank should ensure that appropriate logical access controls to data, Systems, Application software, utilities, telecommunication lines, libraries, System software, etc. are in place.The Internet Banking Infrastructure should be hosted in a secure DMZ. Unnecessary services such as File Transfer Protocol, Telnet etc. should be disabled.In addition, the Internet Banking Application server should be segregated from the E-Mail server.Internet Banking Applications should not be vulnerable to attacks such as “Parameter Tampering”.Real-Time alerts should be sent to the customers regarding any major change in the account/customer profile. E.g. change of beneficiary or mobile number.The contact information (e.g. mobile number, email address) of the customers should be managed from the Core Banking System and linked with Internet Banking Application.Internet Banking Applications should have a feature to identify disabled and dormant accounts. Internet Banking logging in for such accounts should be reactivated with appropriate controls.Internet Banking Applications should have:<ul style="list-style-type: none">➤ Fraud detection feature,➤ Detect the customer usage pattern➤ Identify the geo-location of each transactionIf the transaction pattern is odd or the geo-location is atypical or odd the system should have the facility to inform the customer.Internet Banking Applications should provide the feature of a Virtual Keyboard.Internet Banking Applications should be secured with HTTP Strict Transport Security (HSTS). HSTS is a security measure that relies on the server sending a special response header. This forces the browser (if the browser supports this) to prevent requests from being sent through HTTP for that domain. So, the main difference between HTTPS and HSTS is on the client side.



SN	Procedures
	<ul style="list-style-type: none">The Internet Banking application should support two-factor authentication for login and while performing critical transactions/activity.
6.	Log Monitoring and Intrusion Detection / Prevention
	<ul style="list-style-type: none">All computer accesses, including messages received, should be logged. Security violations (suspected or attempted) should be recorded and follow-up action should be taken.The Bank should also implement effective safeguards such as Next Generation Firewalls, IDS, IPS etc. to prevent intrusion into the infrastructure/network.The Bank should also implement tools for monitoring Systems and networks against attacks and intrusions.The application should have proper record-keeping facilities for legal purposes. It shall be necessary to keep all Received and Sent messages securely.The Firewall should block internet probes and access attempts from blacklisted countries and IP Addresses as provided by RBI circulars.
7.	Periodic Vulnerability Assessment and Penetration Tests
	<ul style="list-style-type: none">The Bank should ensure that security audit and vulnerability assessment and penetration testing is performed before moving Internet Banking and related infrastructure into the production environment and thereafter at regular intervals. This should include Internet Banking applications and associated infrastructure like Server Operating Systems, Web Servers, Databases, Firewalls etc.Attempt to guess passwords using password-cracking tools.Check the known vulnerabilities mentioned in standards such as OWASP-Top-Ten which include Cross-Site Scripting, SQL Injection, Directory Browsing etc.Search for back-door traps in the programs.Attempt to overload the System using Distributed Denial of Service (DDoS) & Denial of Service (DoS) attacks.Check if commonly known holes in the software, especially the browser and the e-mail software exist.The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers').
8.	Adequate Backup Management & Disaster Recovery Controls
	<ul style="list-style-type: none">The Bank should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure that the recovery process meets the business requirements of the Recovery Point Objective (RPO) and Recovery Time Objective (RTO).



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेड्युलड बँक)

SN	Procedures
	<ul style="list-style-type: none">Business continuity should be ensured by setting up Disaster Recovery sites.These facilities should also be tested periodically.
9.	Application Security Controls
	Please refer to the “Application Security Procedures”
10.	Database Security Controls
	Please refer to the “Database Security Procedures”
11.	Operating System Security Controls
	Please refer to the “Operating System Security Procedures”
12.	User Access Management Controls
	Please refer to the “User Access Management Procedures”
13.	Password Management Controls
	Please refer to the “Password Management Procedures”
14.	Data Backup, Recovery & Retention Controls
	Please refer to the “Data Backup, Recovery & Retention Procedures”
15.	Change Management Controls
	Please refer to the “Change Management Procedures”
16.	Log Management and Monitoring Controls
	Please refer to the “Log Management and Monitoring Procedures”

Responsibilities

- IT Infrastructure team
- Administration department

xxxxxx End of Policy Documents xxxxxx



6. Mobile Banking Security Policy

Objectives

The objective of this policy is to establish procedures for safeguarding The Bank's Mobile banking infrastructure from various vulnerabilities & risks.

Scope

This policy is applicable to all geographical units of The Bank and to all the employees, contractors, consultants, partners and third parties.

Policy Statement(s)

1. Procedures shall be established for risk mitigation in mobile banking.
2. Procedures shall be established to ensure that appropriate authentication & encryption controls are in place.
3. Procedures shall be established to ensure that appropriate intrusion prevention controls are in place along with controls pertaining to periodic testing.
4. Procedures shall be established to ensure physical access controls.
5. Procedures shall be established to ensure the confidentiality of customer data.
6. Procedures shall be established for Database Security Controls
7. Procedures shall be established for Operating System Security Controls
8. Procedures shall be established for User Access Management Controls
9. Procedures shall be established for Password Management Controls
10. Procedures shall be established for Data Backup, Recovery & Retention Controls
11. Procedures shall be established for Change Management Controls
12. Procedures shall be established for Log Management and Monitoring Controls

Procedures

SN	Procedures
1.	Risk Mitigation in Mobile Banking The Bank shall put in place appropriate risk mitigation measures like transaction limit (per transaction, daily, weekly, monthly), transaction velocity limit, fraud checks, AML checks etc. depending on The Bank's own risk perception unless otherwise mandated by the RBI. The Bank shall follow the Security Standards appropriate to the complexity of services offered, subject to following the minimum standards as described in this document. The guidelines should be applied in a way that is appropriate to the risk associated with services provided by The Bank and the system which supports these services.
2.	Authentication and Encryption Controls



SN	Procedures
	<ul style="list-style-type: none">The Mobile banking application should be allowed to be installed only on non-rooted/non-jail-broken devices.All mobile banking transactions involving debit to the account shall be permitted only by validation through two-factor authentication.One of the factors of authentication shall be mPIN or any higher standard.Where mPIN is used, end-to-end encryption of the mPIN should be ensured.The mPIN shall be stored in a secure environment.For mobile banking facilities which do not contain the phone number as identity, a separate login ID and password should be implemented to ensure proper authentication.The appropriate level of encryption and security should be implemented at all stages of the transaction processing. As a best practice, end-to-end encryption of the mobile banking transaction should be ensured through application-level encryption and transmission encryption. (TLS)
3.	Intrusion Prevention and Periodic Testing
	<ul style="list-style-type: none">The Bank should establish appropriate firewall rules, intrusion detection systems (IDS), data file and system integrity checking systems, surveillance and incident response procedures and containment procedures.The Bank shall conduct risk management analysis, security vulnerability assessment of the application and network etc. at least once a year.Mobile banking applications should be checked for known vulnerabilities mentioned in standards such as OWASP Mobile Top-Ten which includes insecure platform usage, insecure data storage, insecure authentication etc.The Bank shall maintain proper documentation of security practices, guidelines, methods and procedures used in mobile banking and payments systems and shall keep them up to date based on the periodic risk management, analysis and vulnerability assessment which are being carried out.
4.	Physical Access Controls
	<ul style="list-style-type: none">The Bank shall implement appropriate physical security measures to protect the system gateways, network equipment, servers, host computers, and other hardware/software used from unauthorized access and tampering. The Data Centre of The Bank and Service Providers should have proper wired and wireless data network protection mechanisms.
5.	Ensuring the confidentiality of customer data
	<ul style="list-style-type: none">The mobile banking application should not request unwanted, unnecessary permissions such as access to the camera, contacts SMS, storage etc.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेट शेड्युलड बँक)

SN	Procedures
	<ul style="list-style-type: none">The dependence of The Bank on mobile banking service providers may place knowledge of The Bank systems and customers in the public domain. Mobile banking systems may also make The Bank dependent on small firms. It is therefore imperative that sensitive customer data and the security and integrity of transactions are protected. It is necessary that the mobile banking servers at The Bank's end or at the mobile banking service provider's end, if any, should be certified by an accredited external agency.In addition, The Bank should conduct regular information security audits on the mobile banking systems to ensure complete security.
6.	Database Security Controls
	Please refer to the "Database Security Procedures"
7.	Operating System Security Controls
	Please refer to the "Operating System Security Procedures"
8.	User Access Management Controls
	Please refer to the "User Access Management Procedures"
9.	Password Management Controls
	Please refer to the "Password Management Procedures"
10.	Data Backup, Recovery & Retention Controls
	Please refer to the "Data Backup, Recovery & Retention Procedures"
11.	Change Management Controls
	Please refer to the "Change Management Procedures"
12.	Log Management and Monitoring Controls
	Please refer to the "Log Management and Monitoring Procedures"

Responsibilities

- IT Infrastructure team
- Administration department

• xxxxxx End of Policy Documents xxxxxx



7. Virus Protection Policy

Objectives

The Anti-Virus Policy is designed to ensure that

- Anti-Virus Software is installed on all Servers, Personal Computers, Laptops, E-Mail Servers, Proxies and Internet gateways.
- Only licensed and authorized AV software is being used.
- Any external device should be scanned before allowing it on the Network.
- An incidence response procedure is defined in case of a virus attack on the set-up.

Scope

This policy is applicable to all geographical units of The Bank and to all the employees, contractors, consultants, partners and third parties.

Policy Statement(s)

1. Procedures shall be established for the selection of Anti-Virus Software
2. Procedures shall be established for ensuring proper vendor support
3. Anti-Virus Software shall be installed on all servers and workstations
4. Procedures shall be established for ensuring proper anti-virus infrastructure
5. Anti-virus server configuration shall be documented
6. Anti-virus agent configuration shall be documented
7. Procedures shall be established for virus scans
8. Procedures shall be established for event logging
9. Review procedures shall be established
10. Procedures shall be established for controls over development and test environments
11. Anti-Virus Software shall be installed on all mobile computing devices of The Bank
12. Procedures shall be established for third-party laptops connecting to The Bank's network
13. Procedures shall be established for reporting virus infections
14. Procedures shall be established for handling virus incidents
15. Procedures shall be established for ensuring appropriate Anti-Virus awareness among the users
16. Procedures shall be established for controls over mobile code



Procedures

SN	Procedures
1.	Selection of the Anti-Virus Software Selection of the Anti-Virus (AV) software is a critical decision and should be taken considering the following factors. The Anti-Virus (AV) Software should be able to: <ul style="list-style-type: none">• Be deployed from a central AV Server on all the servers, desktops, internet proxies and gateways, E-Mail servers etc.• Identify and eradicate all known viruses and their variants• Send alerts to the user and administrators about any infections• Able to get update releases in a timely manner as per the SLA Terms and Conditions.• Scan memory, floppies, removable media, USB drives, local and network drives, BIOS, e-mails and attachments, internet browsing and downloads etc.• Should have adequate controls to ensure against modifications except by the authorized AV Administrators.
2.	Vendor support The Information Security Committee (hereinafter referred to as ISC) should ensure that an appropriate Service Level Agreement (SLA) is entered into with the AV Vendor covering the following clauses <ul style="list-style-type: none">• Intimations about any virus outbreaks.• Updates / new signatures should be made available no later than one day.• Intimation about the intermediate compensating control measures to be taken before the updates/signatures for a new virus is released.• In case of a virus infection in The Bank network, the vendor should support eradication.
3.	AV Software is to be installed on all servers and workstations The ISC should ensure that the AV software is installed on all the servers and workstations used for running the applications including all departments, the Help Desk and administrator workstations.
4.	Anti-Virus Infrastructure Approved Anti-virus software shall be configured in a client-server mode to safeguard The Bank network from viruses, Trojan Horses and other malicious software. For this, the following activities must be performed:



SN	Procedures
	<ul style="list-style-type: none">A server hosting the e-Policy Orchestrator (EPO) application shall be installed in the Akola HO.An anti-virus agent shall be installed on all the desktops, laptops and servers connected to The Bank network. This will assist in the integration of all the workstations with the Anti-virus server.IT Systems Administrator shall be responsible for all the activities carried out on the anti-virus application and for ensuring the safety of The Bank network from any virus attacks.All incoming and outgoing shall be scanned at email and SMTP servers for Malware. Email containing malicious codes are cleaned and if the cleaning fails the mail shall be deleted with notification to recipient.To minimize the possibility of malicious code spreading from email attachment, the concern file attachment is blocked from the email and SMTP server.
5.	Anti-Virus Server Configuration
	<p>The Anti-virus server shall be configured to include the following parameters:</p> <ul style="list-style-type: none">Scan Engine, Anti-Virus software patch and antivirus product upgrade shall be done manually to the EPO server.EPO shall be configured to 'PULL' the latest virus definition files (DAT) from the Anti-virus website of the vendor and 'PUSH' these to the workstations connected to the Anti-virus server.The ability to disable anti-virus protection shall not be made available on the Anti-virus agents.
6.	Anti-Virus Agent Configuration
	<p>Anti-virus agents shall be configured to include the following parameters:</p> <ul style="list-style-type: none">To start executing immediately after the system start-up.To download virus definition files.Scan all the external storage devices connected to the server or workstation for viruses and other malicious software.Scan the storage media on the server/workstation every day during non-business hours.Deny users the ability to stop the anti-virus scan initiated during non-business hours.Ability to update virus definition files through Live Updates.
7.	Virus Scans
	<p>The Systems Administrator shall configure the following scans on the anti-virus agents:</p>



SN	Procedures
	<ul style="list-style-type: none">• A Floppy Scan to check the compact disks and other removable media for any malicious software.• A Custom Scan every day to scan all the executable files residing on the storage devices attached to the server/workstation.• A Quick Scan every day to scan the storage devices for any traces of virus and security risks (such as adware and spyware). In the event of any finding, a full scan shall be performed.• A Full Scan every week to scan all the files and folders available in the storage devices.
8.	Event Logging
	<p>The Systems Administrator shall configure 'Event logging' to capture the following:</p> <ul style="list-style-type: none">• Threats History• Scan History• Other activities such as Download Anti-virus definitions, Starting and stop of anti-virus agents etc...• Enable logging of any event which is aimed at tampering with the security settings of the anti-virus agent• All logs generated for the events identified above shall be configured to be stored for 180 days. Every month, the Systems Administrator shall ensure that these logs are archived for review.
9.	Review Procedures
	<p>On a daily basis, the Systems Administrator shall review the Anti-virus server console to verify the following:</p> <ul style="list-style-type: none">• All the desktops, laptops and servers in The Bank network shall be connected to the Server application• All the virus definition files loaded with the anti-virus agents are up-to-date• All the scheduled scans are carried out as per the defined schedule scans• Desktops, laptops and servers not updated automatically should be updated manually• In case of any discrepancies, the Systems Administrator must ensure immediate remedial measures.• On a monthly basis, the logs generated by the Anti-virus agents shall be reviewed by the Systems Administrator to identify the threats and the quarantined files of each workstation. The details of these reviews shall be communicated to the IT Manager.



SN	Procedures
10.	Controls over the Development and Test environments
	<ul style="list-style-type: none">The Application Service Provider who is engaged in the development and maintenance must ensure that any patches, fixes, upgrades etc. released are virus free.When delivered to The Bank, these new programs should be tested for functionality as well as checked for viruses.AV software in the test and development environments must be kept up-to-date with the latest signatures.
11.	AV on mobile computing devices like laptops
	<ul style="list-style-type: none">The ISC should set up a process of installing and keeping up-to-date, AV software on all laptops.The owner/custodian of the laptop should sign an undertaking to the effect that he will surrender the laptop at certain intervals for the AV updates.
12.	Third-Party Laptops
	<ul style="list-style-type: none">Third parties should not be allowed to connect their laptops to The Bank Network.If it is necessary, then the laptop must be scanned for viruses with the approved AV Software before allowing it on the network.
13.	Reporting of Infection
	The ISC should inform all users of the contact details (phone number, e-mail IDs etc.) of the identified administrators and ISC members for reporting any virus-like activity.
14.	Handling Virus Incident
	<ul style="list-style-type: none">As and when new malicious code is reported that uses specific port/s and website/s, the concerned port/s and website/s are blocked at the router and firewallIn case the computer is detected with Spyware by the EPO server, the Network and Internet connectivity of the computer shall be disabled immediately. IT engineer shall clean the spyware immediately and if it cannot be cleaned the system should be rebuilt after formatting.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेड्युलड बँक)

SN	Procedures
15.	User Education
	<p>The ISC should ensure that the users are given adequate training on the following</p> <ul style="list-style-type: none">• Users should use only The Bank approved workstations and software.• Users should ensure that the AV software on their workstation is up-to-date. For this, the users shall review the last date of the virus definition file update, if there is a delay in the update, the details shall be communicated to the IT Helpdesk.• Users must not attempt to change the setting of the AV software.• Users must not install freeware, downloaded or unapproved software.• Users shall not download any emails with unknown senders, attachments and formats.• Users should be given training to Identify and report any abnormal activity on the workstations e.g. abnormal delay in opening files, loss of files, unusual displays on the screen, AV software displaying virus infection messages on the screen etc. In the event of any unusual activity, the details shall be immediately conveyed to the IT helpdesk, who must in turn communicate with the IT Manager.
16.	Controls over mobile code
	<p>Mobile code is software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction. Mobile code is associated with a number of middleware services.</p> <ul style="list-style-type: none">• Only authorised mobile codes should be allowed to be executed• Mobile Code should be tested to ensure that it does not contain any malicious code

Responsibilities

- Various departments of The Bank
- Manager-IT
- IT Support Team

xxxxxx End of Policy Documents xxxxxx



8. Data Backup, Recovery and Retention Policy

Objectives

- Backups of the Infrastructure like Operating Systems, Applications, databases, interfaces, and other utilities are available, in case of failure of the production environment.
- The Bank should ensure that the backups are tested for restoration at regular intervals.
- The Bank should define the retention period for backups and store them in a secure manner.
- The Backup media is appropriately labelled.
- The Infrastructure Service Provider should maintain an inventory of the Backup media.
- The Backup media is recycled and not used after it is rewritten the vendor-defined number of times. This will ensure Backup media failures.

Scope

This policy is applicable to all geographical units of The Bank and to all the employees, contractors, consultants, partners and third parties.

Policy Statement(s)

1. High-Level guidelines for backup shall be defined.
2. Responsibility for defining backup shall be established.
3. Procedures shall be established for defining backup requirements.
4. Procedures shall be established for the encryption of backups.
5. Procedures shall be established for changes to the backup requirements.
6. One nodal person shall be appointed for backup activities.
7. Appropriate vendor support shall be ensured.
8. Every new backup request shall be approved by IT Manager or any other person nominated for the purpose.
9. Backup responsibility shall be established.
10. Procedures shall be established for temporary backups.
11. Procedures shall be established for the review of backups.
12. Procedures shall be established for documentation and records.
13. Media supplied by the vendor shall be as per the requisition made. The media shall be in sealed packed condition before it is accepted.
14. Whenever there is in need for backup media, IT Department will take the approval from IT Manager and procure the media and update the records in the inventory.



15. Procedures shall be established for the labelling of backup media.
16. Procedures shall be established for maintaining an inventory of backup media.
17. Procedures shall be established for choosing backup media and backup applications.
18. Procedures shall be established for the rotation/recycling of backup media.
19. Backup tapes shall be stored in a cool and dust-free environment as per the specifications of the Backup Media Vendor.
20. Backup Tapes shall be stored in Fire Resistant cabinets.
21. Controls over the movement of tapes shall be established.
22. An up-to-date backup register shall be maintained.
23. The restoration procedure shall be defined.
24. Procedures shall be established for testing of backup.
25. Procedures shall be established for testing complete re-storability / recoverability.
26. Procedures shall be established for retiring backup media.
27. Procedures shall be established for the physical destruction of retired (faulty) media.
28. Backup and recovery-related tasks shall be defined.
29. Review procedures shall be established.

Procedures

SN	Procedures
1.	High Level Guidelines for Backup
	<p>The high-level guidelines for taking the data backup are as follows:</p> <ol style="list-style-type: none">1. Important backup data information shall be collected, which need to be scheduled for daily backup.2. Backup activities shall be implemented after the day end on working days. If a complete or weekly full (WF) backup cannot be taken for any unforeseen reason, it is taken on the next working day.3. As per Bank's IT department requirement (DF- WF) backup policy is finalised after discussion with IT Manager. This policy can only be altered after necessary approval from IT Manager.4. For DF – WF backup strategy:<ul style="list-style-type: none">➤ Daily full (DF) backup shall be conducted on Monday, Tuesday, Wednesday, Thursday, Friday and Saturday on two Tapes/Media➤ All successful or unsuccessful scheduled backup status shall be entered in the Backup Log File (Ref... Daily Backup Log Report) with the appropriate reason.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपेटिट शेड्युलड बँक)

	<p>5. Offsite Backup: One set of backups shall be kept at ESDS location and other at AUCB, HO) on daily basis.</p> <p>6. Monthly Backup:</p> <ol style="list-style-type: none">The backup of the last week of the month shall be called a monthly backup.2 sets of monthly backups shall be taken.One set shall be at ESDS Nashik and the second set shall be Kept at The Bank's Head Office in Akola.The monthly backups of June, September and December shall be maintained as quarterly backups. One set shall be at ESDS Nashik and the second set shall be sent to other location in Head Office.The monthly backup of March shall be maintained as a Yearly backup. One set shall be at ESDS Nashik and the second set shall be at The Bank's Head Office in Akola. <p>7. All three types of backup activities shall be fairly identical for any given system. However, off-site backups shall differ – here, the tapes shall be collected before the backup has started and subsequently returned after the process has been completed.</p> <p>8. Once the backup is taken, and the log is updated, the Backup Log shall be filled by the person conducting the activities stated in this procedure.</p> <p>Monthly and Quarterly Backup tapes shall be retained as per RBI requirements.</p>
2.	Responsibility of defining backup
	<p>Owners of the information assets like operating systems, databases, applications, network components and other information assets should identify the data to be backed up.</p> <p>The information asset owners will decide appropriate backup plan, taking into consideration its importance to the business, legal requirements and technology available.</p>
3.	Defining Backup Requirements
	<ul style="list-style-type: none">Name and contact details of the owner of the assetName and contact details of the custodian OR coordinator (appointed by the owner) of the asset for all backup related activitiesNew requirement / change in existing backup requirementThe details of servers / drives / folders / files to be backed upThe frequency of backups (daily, weekly etc.)



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेड्युलड बँक)

	<ul style="list-style-type: none">• Whether local backup required (on a separate Hard Disk/Tape)• The type of backup (incremental / differential / full backup etc.)• Number of sets – One or Two• Whether storage at off site is required• State of the Database to be backed up (Cold, Warm, Export, etc.)• The retention periods• Whether data needs to be encrypted or not
4.	Encryption of backups
	The information asset owners should decide appropriate encryption, taking into consideration its importance to the business, legal requirements and technology available.
5.	Changes to the backup requirements
	Every change/modification should be intimated by the user immediately for which the same procedures would be followed as stated above as the change or modification related to backup will be treated as new backup request. All such change management should be duly approved/ authorized by IT Manager or person nominated by IT Manager.
6.	Appointing one nodal person
	The nominated business user (custodian/coordinator) should coordinate all backup and restoration related activities.
7.	Vendor Support
	Where necessary the IT department should organize appropriate support from the Application and Database Vendor/s, to set up the backup for an assured recovery.
8.	Approval of the Backup Request
	Every new backup request should be approved by IT Manager or any other person nominated for the purpose.
9.	Backup Responsibility
	Two database backups are performed every day. One is taken by The Bank at the time of “day seal”. One copy of the latest backup is available with The Bank. The second backup is performed by ESDS (Auto Backup) at Nashik every day. Backups of the other supporting infrastructure like the database and server operating systems is performed by ESDS at Nashik.



	<p>Generally, the Server room will use Centralized backup solutions for scheduling and taking backups. Only where specifically required by the business, separate media backup will be allowed.</p> <p>The required resources should be made available before approving any backup request. The resources can be in the form of server space, local backup device, etc. In case of any problem, the IT Manager should take decision on how to go ahead on backup for a particular request.</p>
10.	Temporary backups
	<p>Temporary backups may be allowed on a case-to-case basis e.g. taking backup of a laptop which is to be sent out for repair.</p>
11.	Review of backups
	<p>Every six months the backup team head should intimate the respective project heads about the current strategy for backups, which will be reviewed by the Business head who may put forth changes that may be required including discontinuation of the backups.</p>
12.	Documentation and Records
	<p>The backup plan with schedule should be documented and should be available for reference and verification with the information asset owner and the team responsible for the execution of the backup schedule.</p> <p>The backup plan should also identify the reporting procedures for the execution of the backup schedule and problems encountered.</p> <p>Wherever possible automated logs should be generated for the backup activity and exceptions should be reported to the information owner without exception.</p> <p>The logs of backup activity (either automated or manual) should contain details like:</p> <ul style="list-style-type: none">➤ Directories and files backed up➤ Operator name➤ Success or failure <p>Failures in backups are exceptions and must be reported to the information owner giving brief description of the problem and the status of correction</p>
13.	New Backup Media
	<p>Media supplied by vendor should be as per the requisition made. The media should be in sealed packed condition before it is accepted.</p>
14.	Issuing New Backup Media
	<p>Whenever there is in need of backup media, IT Department will take the approval from IT Manager and procure the media and update the records in the inventory.</p>



15.	Labelling of Backup Media
	Each backup taken should be labelled in a manner that will help identify the correct media for restoration without ambiguity. A standard policy for labelling the backed-up media is followed which is as “Week Day” i.e. Monday.
16.	Inventory of Backup Media
	A complete inventory must be maintained of <ul style="list-style-type: none">• The media used for backups• Unused media (blank), Cleaning Tape Media• Media identified for destruction
17.	Choice of backup media and backup application
	<p>Choice of backup media should be guided by considerations like</p> <ul style="list-style-type: none">• size of data to be backed up• requirements of backup application• speed of backup & restoration process• data retention requirement• the expected life of storage media itself• reliability requirements• available technology <p>Specific data storage architectures i.e. Storage Area Network (SAN) sub-systems may be connected to production servers if necessary. In this regard, the architecture and connectivity of sub disk storage systems should reviewed for single points of failure and fragility in functional design and specifications, as well as the technical support by service providers.</p>
18.	Rotation/recycling of backup media
	<p>Backup media should be rotated ensuring that</p> <ul style="list-style-type: none">➤ Adequate numbers of generations of backups are available.➤ That no media is recycled (reused for taking backups) beyond 'number of writes' as prescribed by the vendor of the media.
19.	Storage of Backup Media – environment
	Backup tapes should be stored in a cool and dust free environment as per the specifications of the Backup Media Vendor.
20.	Storage of Backup Media
	The Backup Tapes should be stored in Fire Resistant cabinets.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेड्युलड बँक)

21.	Controls over movement of Tapes
	<p>Backup media should be transported in waterproof and tamper proof Metallic box, having locking facility</p> <ul style="list-style-type: none">• Movement of media to and from the off-site location must be recorded in such a manner that each media is traceable• Movement of media should be authorized by the information owner• Movement of media should be done only by the identified person or through the identified agency• Keys of the metallic box containing the backed-up media, must not be given to the carrier.
22.	Backup Register
	<p>A backup register should be maintained giving various details like name of the system backed up, date of backup, type of backup, backup media type and number, Number of writes for that media, retention period etc.</p>
23.	Restoration Procedure
	<p>Backup restoration activity is carried out after every backup. Random data from the common folder selected and restored on log folders to ensure that data is intact. Test Restoration shall be carried out on a monthly basis and this shall be recorded in 'Test Backup Restore Form'.</p> <p>For any restoration request of any data to be restored, a form of 'Data Backup Restoration Request' is duly filled by the concerned user and it is signed / approved by the Department and IT Manager.</p>
24.	Testing of Backup
	<p>Backup should be tested for its readability and restorability at regular intervals. The intervals for such testing should be as per the backup plans prepared by the information owner.</p> <p>The Application coordinator / custodian should initiate restoration requirements.</p>
25.	Testing complete restorability/recoverability
	<p>The Bank with the help of ES/DS performed tests readability and restorability of the backups.</p> <p>While carrying out a full restoration / recovery following things should be considered</p> <ul style="list-style-type: none">• Convenient timing of the test restoration / recovery• Restoration should be done only in a test environment.• Restoration should be possible only for those files which are selected



	<ul style="list-style-type: none">• Restoration should be possible with the original (as in production) set of directory and file permissions• Should be witnessed by Information Owner.• The Information Owner should document the test results. <p>If any problems are encountered during test restoration, then the backup plan / procedures should be suitably modified. The modified / revised test restoration / recovery should be scheduled immediately to confirm that they restoration happens as desired.</p> <p>After the test restoration / recovery is complete, the restored data should be removed</p>
26.	Retiring of Backup Media
	<p>It is very important to discard the media from the backup cycle after vendor recommended read/write operations have been reached.</p> <p>The following procedure is followed to reject / discard any media from the cycle:</p> <ul style="list-style-type: none">• Physically damaged Media• Any error occurred while read / write operation on Media. Faulty media are discarded immediately after it is authorized by IT Manager.• Vendor recommended read/write operations have been reached
27.	Physical Destruction of Retired (faulty) Media
	<p>The backup media should be destroyed</p> <p>After confirming that the media has really gone bad or really needs to be destroyed</p> <p>After making a record of the media label details and updating the media inventory record which is authorized by the Backup Team Head.</p> <p>In the presence of at least two identified officials who will witness the destruction and sign in the inventory record.</p> <p>Thereafter, the media should be cut into pieces, preferably using special shredders for the purpose.</p>
28.	Backup and Recovery Related Tasks
	<p>Daily Backup Log Report: Backup Administrator shall fill up the Backup Log form with details like tape id, date, type of backup, etc. (Ref. Appendix for Daily Backup Log Report Template)</p> <p>Data Backup Restoration Request Form: Backup Restoration procedure shall start with the respective functional head raising the call with IT Helpdesk for Data Restoration. The backup administrator shall restore the data and close the ticket.</p>



	<p>Users requesting a restore/s shall be required to provide as much information about the data (file/s) as necessary – this will include:</p> <ul style="list-style-type: none">➤ The reason for the restore➤ The name of file/s and/or folder/s to be restored➤ Original location of file/s and/or folder/s - the IT Help Desk shall provide guidance to the User on how to find this out
29.	Review Procedures
	<ol style="list-style-type: none">1. Backup Administrator shall have to put the details for backup and restore in respective templates, shall do report logging (Ref. Daily backup log report).2. IT Manager shall verify the fact-recording sheet with backup systems engineer for specific details.3. Change Management: Email shall be sent by Backup Administrator if any of hardware/software components of existing Backup server needs to be changed/removed/upgraded.4. Change request form shall be used for the change management. This form shall be filled up by the Backup Administrator & duly approved by the IT Manager.5. If a scheduled backup cannot be taken or there is a deviation from the process, it shall be entered in the Log (Ref. Daily Backup Log Report) with the appropriate reason. This shall be also intimated to IT Manager via email.6. Testing of backup data restoration to be carried out as per agreed timelines and Backup Administrator shall carry out the restoration test and enter the required information in the log (Ref. Test backup restoration form)

Responsibilities

- Administrators of various systems – Operating Systems, Applications, Databases, Routers, Firewalls etc.
- Backup Operators

xxxxxxx End of Policy Documents xxxxxx



9. Media Handling Policy

Objectives

The objective of the policy is to

- Ensure that information media is controlled and physically protected.
- Ensure that all media is stored in a safe, secure environment in accordance with manufacturers' specifications
- Develop procedures for secure and safe disposal of media to minimize the risk of sensitive information leakage to unauthorized persons
- Develop procedures for handling, storing, and communicating information consistent with its classification.

Scope

The policy applies to all the information media used / generated / transferred to/from within The Bank and is applicable to all employees, vendors, and agents involved in handling removable media of The Bank.

Policy Statement(s)

1. All types of media used by the branches, departments and offices shall be appropriately labelled.
2. Procedures shall be established for media handling.
3. Procedures shall be established for the security of media in transit.
4. Procedures shall be established for the disposal of media.
5. Procedures shall be established for the storage of media.

Procedures

SN	Procedures
1.	Media Labelling
	All types of media like CDs, Registers, and documents used by the branches, departments and offices shall be appropriately labelled as per Asset Classification and Labelling Policy
2.	Media Handling
	<ul style="list-style-type: none">• All the media shall be stored in the safe and secure environment• Procedure for issuing a CD



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपेटिट शेड्युलड बँक)

SN	Procedures
	<ul style="list-style-type: none">An employee shall drop an email to the Head of the department and IT department stating the purpose and seeking permissionUpon email approval, the IT department will issue the CD to the employee
3.	Media in Transit
	<ul style="list-style-type: none">In case of computer media or any other important document of The Bank is in transit, then the person carrying the same shall be responsible for its security.Reliable transport or a courier agency shall be used. A list of authorized couriers shall be agreed upon with the Management of The Bank and the procedure to check the identification of the couriers shall be implemented.Packaging shall be adequate to protect the contents from any physical damage.All such media shall be recorded in the media transit register.
4.	Disposal of Media
	<ul style="list-style-type: none">Media shall be disposed of securely and safely when no longer required.In the case of records like paper documents, the same shall be destroyed using a paper shredder after the prescribed period of timeIn case of permanent disposal of equipment containing the information shall be irreversibly deleted before the equipment is moved off the site.A separate Disposal of IT Asset Policy (AU-IT-POL-L2-002) was created as per the recommendation in the external IS Audit for the year 2021-22; which can be referred to for more details.
5.	Storage of media
	The documents shall be stored securely at an offsite location for a specified retention time as per Media Handling Policy.

Responsibilities

- Backup Administrators
- IT Support Team

xxxxxx End of Policy Documents xxxxxx



10. Change Management Policy

Objectives

The objective of the policy is to

- The Change Management Policy is designed to
- Ensure that each change is documented, studied for feasibility, approved and tracked till movement into a production environment.
- Each change is tested before moving into a production environment.
- The user and technical documentation is updated for the respective system.
- Provide a mechanism for urgent changes to be carried out in exceptional circumstances.
- Rollback of the change is provided.

Scope

This policy is applicable to all geographical units of The Bank and to all the employees, contractors, consultants, partners and third parties.

Policy Statement(s)

1. Each Change Request with reasoning, module, a problem expected to be resolved etc. must be recorded even if not considered for change.
2. Each change request shall be studied for its feasibility.
3. Priority Number, Criticality and scale of change shall be indicated in the approval.
4. The target date of change requirement shall be decided.
5. Changes shall be tracked.
6. Procedures shall be established for testing by the developer.
7. Procedures shall be established for risk and impact analysis.
8. Procedures shall be established for user acceptance testing.
9. Procedures shall be established for the migration of changes to the production environment.
10. Procedures shall be established for the replication of successful changes.
11. Procedures shall be established for carrying out necessary changes to documentation.
12. Procedures shall be established for the closure of change requests.



Procedures

SN	Procedures
1.	Each Request Must be recorded and numbered
	Each Change Request with reasoning, module, a problem expected to be resolved etc. must be Recorded even if not considered for change. Various other details like the date of request, name of the requester and a running serial number should be given to each request received and tracked till it is closed by movement into the production environment or discarded.
2.	Changes must be studied for feasibility
	Each change request should be studied for its feasibility. There may be a simple workaround available which may produce desired results and the change may not be warranted.
3.	Criticality, priority and scale of change should be studied
	Priority Number, Criticality and scale of change should be indicated in the approval indicating an expected date for closure.
4.	Decide the target date of the change requirement
	The approved request should be given to the vendor / development team for development indicating the date by which the change is required. The vendor / development team should accept the target date for completion.
5.	Changes should be tracked
	Each change request should be tracked to check the progress. A logging facility should be enabled to record activities that are performed during all the phases including migration process of the change requests.
6.	Testing by the developer
	The vendor / development team should complete the development and carry out tests before handing over the new code for User Acceptance Testing.
7.	Risk and Impact Analysis
	Detailed risk and impact analysis of the change request in relation to existing infrastructure, network, and related systems should be performed. It should also be ensured that the introduced change would not create any security implications or software compatibility problems for affected systems or applications.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपेटेट शेड्युलड बँक)

SN	Procedures
8.	User Acceptance Testing
	User Acceptance Testing should be carried out in a separate physical or logical Test Environment before moving the changes to production environment. If rejected, reasons should be documented and given back to the vendor / development team. If the UAT environment needs access to internet, the same should be enabled only after performing a detailed risk assessment.
9.	Migration to Production
	Precautions against malicious codes should be taken during the transition from the UAT environment to the production environment.
10.	Replication
	After a change has been successfully implemented in the production environment, it should be replicated to disaster recovery systems or applications for ensuring consistency.
11.	Changes to the Documentation
	The Custodian should complete the documentation related to the change request, and system documentation and inform the affected users.
12.	Closure and record
	The Change Request should be closed and recorded.

Responsibilities

- Change requests in the CBS are managed by Virmati and the changes to supporting infrastructure like the database and server operating systems is managed by ESDS.
- IT Support Team for workstations at the Branches

xxxxxx End of Policy Documents xxxxxx



11. Security Incident Management Policy

Objectives

The Security Incident Management Policy is designed to

- Establish a process for the management of incidents, malfunctions and abuses.
- Provide guidance to the technical and management users to enable quick, efficient and effective recovery from Incidents.
- To minimize loss from Incidents.
- To carry out a root cause analysis, document and learn from the Incidents and implement controls to arrest the recurrence of the Incidents.

Scope

This policy is applicable to all geographical units of The Bank and to all the employees, contractors, consultants, partners and third parties.

Policy Statement(s)

1. An Incident Response Team (IRT) shall be identified.
2. The IRT shall ensure that various possible incidents / problems are studied and documented including the steps for resolution.
3. Adequate and repeated training shall be given to various users to help them understand and identify an event / incident / problem.
4. Procedures shall be established for incident / problem reporting.
5. Procedures shall be established for incident / problem analysis.
6. Procedures shall be established for the activation of the incident response team.
7. Procedures shall be established for containing the incident / problem and removing the cause.
8. Escalation Process shall be established.
9. Procedures shall be established for root cause analysis.
10. Procedures shall be established for the collection of evidence
11. Procedures shall be established for implementing additional / change of controls.

Procedures

SN	Procedures
1.	Define Incident Response Team
	An Incident Response Team (IRT) should be identified and should comprise the ISC, and administrators of Application / OS / DB / Network. The Incident Response



SN	Procedures
	<p>Team leader should be identified and should be vested with the power to declare and activate the Incident Response Team.</p> <p>The roles and responsibilities of the staff involved in the IRT, including recording, analysing, remediating and monitoring incidents or problems should be clearly defined.</p>
2.	Document the Types of Incidents / Problems and steps for recovery
	<p>The IRT should ensure that various possible incidents or problems are studied and documented including the steps for resolution.</p> <p>Each possible incident or problem along with the steps should be documented and reviewed and rehearsed at regular intervals.</p> <p>The document should be available with the IRT.</p>
3.	Incident / Problem Identification
	<p>Adequate and repeated training should be given to various users to help them understand and identify an event / incident / problem.</p> <p>This would include a demonstration of sirens, alarms, incorrect system behaviour, other indications etc.</p>
4.	Incident / Problem Reporting
	<p>The users should be given informed about the process of incidence / problem reporting, to the appropriate authority for an early resolution.</p> <p>For any incidents which may happen at the CBS environment in Nashik, ESDS will be responsible for resolution and reporting to The Bank</p>
5.	Incident / Problem Analysis
	<p>Incidents / Problems should be assigned appropriate severity levels. As part of incident / problem analysis, incident / problem severity levels should be determined by relevant designated staff members. These staff members should be trained to discern incidents / problems of high severity level. Moreover, criteria used for assessing severity levels of incidents / problems should be established and documented.</p>
6.	Activation of the Incident Response team
	<p>In case of an incident / problem, the head of the Incident Response Team should declare the incident / problem and activate the response team in a timely manner.</p>
7.	Containing the Incident / Problem and removing the cause
	<p>The Incident Response Team should first try to contain the Incident / Problem to ensure that the damages are minimal.</p>



SN	Procedures
	<p>After containment the Incident Response Team should remove the cause of the Incident / Problem.</p> <p>The Team should be careful to safeguard the evidences to help the investigation. The Team should monitor all the incidents / problems and ensure that the timelines for resolution are achieved.</p>
8.	Escalation Process
	<p>Timeframe for the resolution of Incidents / Problems should be commensurate with the severity level and the corresponding escalation process should be defined to ensure timely resolution. These escalation procedures should be tested from time to time to evaluate effectiveness.</p> <p>If an Incident / Problem is likely to develop into a major crisis, senior management should be immediately informed. Thereafter, senior management should take a call about declaring disaster and taking necessary actions thereof. Intimation about such cases should also be given to customers or relevant statutory authorities if applicable.</p>
9.	Root Cause and Impact Analysis
	<p>The Incident Response Team should carry out a root cause analysis of the Incident / Problem to establish the reasons for incident / problem and document the findings.</p> <p>Root Cause Analysis should cover the following:</p> <ul style="list-style-type: none">a. Root Cause Analysis<ul style="list-style-type: none">i. When did it happen?ii. Where did it happen?iii. Why and how did the incident / problem happen?iv. How often had a similar incident / problem occurred over the last 3 years?v. What lessons were learnt from this incident / problem?b. Impact Analysis<ul style="list-style-type: none">i. Extent, duration or scope of the incident / problem including information on the systems, resources, customers that were affected;ii. Magnitude of the incident / problem including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence; andiii. Breach of regulatory requirements and conditions as a result of the incident / problem.c. Correction and Corrective Measures



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेअरहुल्ड बँक)

SN	Procedures
	<p>i. Immediate correction to be taken to address consequences of the incident / problem. Priority should be placed on addressing customers' concerns and / or compensation;</p> <p>ii. Measures to address the root cause of the incident / problem; and</p> <p>iii. Measures to prevent similar or related incidents / problems from occurring.</p> <p>The root cause analysis will help identify the control weaknesses in technology and processes.</p>
10.	Collection of Evidence
	<p>Collecting and preserving evidence and documenting the particulars of an incident / problem is essential for meeting a range of reporting requirements and gathering evidence that may be used in legal proceedings.</p> <p>Evidence should be collected as soon as is reasonably possible and be preserved, documented, and/or tracked by</p> <ul style="list-style-type: none">• Ensuring that the scene of the incident / problem is secured and preserved• Collecting physical evidence and observing a strict chain of custody protocol• Conducting interviews• Collecting any other documentation relevant to the incident
11.	Implementing additional / change of controls
	<p>The IRT and the leader will review the root cause analysis and the weaknesses and define changes (including additional controls) to the technical and / or procedural controls to ensure the recurrence of such incidents or problems.</p>

Responsibilities

- For any incidents which may happen at the CBS environment in Nashik, ESDS will be responsible for resolution.
- IT Support Team

xxxxxxx End of Policy Documents xxxxxxx



12. Log Management & Monitoring Policy

Objectives

This Policy is developed to ensure that

- Audit Trails / Logs capture adequate details like the user ID, Activity of the user, the location identifier and the Date and Time Stamp to ensure accountability.
- System Logs should help in analysing the performance and other issues.
- Audit Trails / Logs are secured against unauthorized modifications.
- The time stamping of logs should be done with the network time server (Clock Synchronization)
- Audit Trails / Logs should be retained for the defined period.
- A process of analysing and monitoring the logs to identify security incidents and operational problems is defined and implemented.

Scope

This policy applies to all logs generated by the application systems, Database, operating systems, and network components, including the physical access logs maintained in manual registers and surveillance systems.

Policy Statement(s)

1. Log management strategy should be defined.
2. The logs should capture the necessary details.
3. Procedures should be established for log analysis.
4. Adequate disk space should be maintained all the time on respective systems for storing logs.
5. Common network time stamping should be used.
6. The Log files should be access controlled.
7. All Log files should be opened in Append mode.
8. Logs should be preserved for a period as defined by the ISC.
9. In the case of investigations, the log files should be preserved for the required period as determined by the ISC.
10. Log host should be defined.
11. Installation logs should be backed up and then removed from the system.



Procedures

SN	Procedures
1.	Log Management Strategy
	<ul style="list-style-type: none">A Log/audit trail strategy should be designed, documented and implemented to help ensure that the logs are enabled, stored securely, analysed, monitored, accountability established, etc.Audit Trails / Logs should be enabled on the Application and all supporting Infrastructure components like Databases, Operating Systems, Web Sphere, Switches, Routers and Firewalls.Logs / Audit Trails should be implemented for access to critical areas like Data Center, Power Supplies, Air Conditioning Units etc.
2.	Capturing necessary details
	The logs should capture details like user Id, Location, activity and date and time to establish accountability.
3.	Log Analysis
	<ul style="list-style-type: none">Logs help analyse and monitor the system performance, errors, security events, switching of users, login-logout, access failure, user activities, backup activities etc.The Bank should set up a process to review and monitor the logs at regular intervals. E.g. the logs that should be captured, analysed and monitored are network traffic logs, E-Mail logs, OS/DB logs, application logs etc.
4.	Enabling logs – Ensuring adequate disk space
	To ensure that logging does not stop, adequate disk space should be maintained all the time on respective systems.
5.	Enabling logs – Common Network Time Stamping
	To ensure correct analysis of the logs, a common network time tamping should be used.
6.	Enabling logs – Strict Access Controls over Log Files
	The Log files should be access controlled to ensure against unauthorized modifications. Where possible the logs should be enabled in Binary mode.
7.	Enabling logs – Logs Files in Append Mode



SN	Procedures
	All Log files should be opened in Append mode to ensure that the earlier logs are not overwritten.
8.	Retention Period for Logs
	Logs should be preserved for a minimum of over 180 days period and defined by the ISC for various Information Assets.
9.	Retention Period in case of an investigation
	In case of investigations, the log files should be preserved for the required period as determined by the ISC considering the applicable regulatory guidelines.
10.	Log Host to be defined
	<ul style="list-style-type: none">All user activities must be logged by the Operating Systems, Applications, Software, Databases, Network Elements and telephony devices whichever is applicable. In case, logging degrades the performance of the systems, only restrictive logging and monitoring of critical commands/ activities can be configured.The Log host should be under the administrative control of a different group rather than the IT Administrator e.g. the log host may be under the Security Group
11.	System Installation Logs
	Installation logs should be backed up and then removed from the system, since they may contain installation user IDs and passwords.

Responsibilities

- Administrators of various systems – Operating Systems, Applications, Databases, Routers, Firewalls etc.

xxxxxxx End of Policy Documents xxxxxxxx



13. Personnel Security Policy

Objectives

The objective of this policy is to establish procedures aimed at protecting the corporate assets of The Bank from intentional misuse, abuse or damage by the employees of The Bank.

Scope

The objective of this policy is to establish procedures aimed at protecting the corporate assets of The Bank from intentional misuse, abuse or damage by the employees of The Bank.

Policy Statement(s)

1. Procedure for carrying out detailed pre-employment checks of short-listed candidates shall be established.
2. Procedures shall be established for carrying out other checks.
3. Procedures shall be established to ensure staff vigilance.
4. Non-Disclosure Agreements shall be obtained before the commencement of employment.
5. All the employees shall be trained to identify any conflicts of interest.
6. Appropriate awareness training shall be given to the users.
7. Procedures shall be established for technical training to senior / middle-level management as per requirements.
8. Procedures shall be established for cyber security awareness training to stakeholders / senior management / board.
9. Responsibility Matrix for various operations including those relating to information security shall be defined and maintained.
10. Procedures shall be established for the return of Assets - Termination / Resignation of the employee.

Procedures

SN	Procedures
1.	Pre-employment checks
	It is the responsibility of the HR department to formulate a procedure for carrying out detailed pre-employment checks of short-listed candidates and verify that candidates have the necessary credentials for employment. In performing these checks, it should become clear whether applicants have concealed important



SN	Procedures
	information about themselves. Depending on the role, the HR department should perform other checks in order to assess an individual's knowledge, educational qualifications, experience, integrity, reliability and character. These checks would also include face-to-face interviews and personality trait identification.
2.	Staff vigilance
	The HR department should ensure that the staff members of The Bank are fully aware of issues surrounding terrorism. It is important to maintain a healthy and active dialogue with staff members in order to discuss potential threats and concerns and to highlight suspicious attitudes and behaviour from co-workers.
3.	Non-Disclosure Agreements
	All employees of The Bank should sign a Non-Disclosure Agreement as per the pre-defined and approved format. This form should be signed before the commencement of employment.
4.	Conflict of interest
	All the employees should be made aware of any conflicts of interest to minimize acts that may harm The Bank's assets and reputation.
5.	Disciplinary Processes
	HR Department should have a disciplinary process in place for violation of The Bank's cyber and information security policies and procedures and any other information security breaches.
6.	Security Awareness for users
	Appropriate awareness training in layman's language should be given to the users, about The Bank's Cyber and Information Security Policies and Procedures. Contents of such training should be reviewed at least once a year and should be approved by the security committee. Such training should be given at least once a year to all the users including existing and new employees as well as resources from vendors / third parties having access to The Bank's information assets. More details are provided in this document in a separate 18. Information Security Awareness Policy .
7.	Technical Competence Training to Senior / Middle Management
	HR Department in consultation with IT Department, should conduct periodic assessments of the IT training requirements for senior and middle management to ensure that sufficient, competent and capable human resources are available.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेट शेड्युलड बँक)

SN	Procedures
	Based on the findings of such assessments, necessary training should be conducted for senior and middle management.
8.	Cyber Security Awareness for Stakeholders / Senior Management / Board
	HR Department in consultation with IT Department, should conduct periodic cyber security awareness training for all the users of The Bank. This training would cover staff at all levels. Senior Management and Board Members of The Bank should be given appropriate awareness about various threats related to cyber security. This training should create appropriate cyber security awareness among the customers of The Bank (if applicable), vendors, service providers and other relevant stakeholders of The Bank about their cyber resilience objectives.
9.	Responsibility Matrix
	HR Department should define and maintain a Responsibility Matrix for various operations including those relating to cyber and information security.
10.	Return of Assets - Termination / Resignation of the employee
	<ul style="list-style-type: none">The HR department should establish a clearance process to ensure that when an employee resigns, all physical access codes are deactivated or changed and badges, keys, etc. are returned before the employee leaves the premises.Depending on the nature of the termination, the former employees should be subject to varying levels of observation and escort. All materials that an employee wishes to remove from the premises should be inspected.Employees are equally responsible for returning all badges, keys or other materials on termination of service.

Responsibilities

- Human Resource Department

xxxxxxx End of Policy Documents xxxxxxx



14. Physical and Environmental Security Policy

Objectives

Recently The Bank has migrated its' critical hardware infrastructure such as Servers, Firewalls etc. to the Managed Data Centre and Cloud Hosting Services Provider "ESDS – Nashik". At ESDS appropriate Physical and Environmental (P&E) controls are implemented. With this, the earlier P&E controls related to The Bank's data Centre at Akola HO have become redundant.

Now, only the non-critical hardware infrastructure is remaining with The Bank. The Bank has redefined the Physical and Environmental Security Policy. The primary objective of P&E controls continues to remain the same as earlier i.e. to reduce the risk of loss, theft, damage, or unauthorized access to The Bank's resources, or interference with The Bank premises and information.

Scope

This policy is applicable to all Branches and offices of The Bank and to all the users including employees, contractors, consultants, partners and third parties.

Policy Statement(s)

1. Identification badges should be worn by the users when at work
2. Procedures for temporary / lost / stolen identity badges shall be established
3. Controls over visitor entry
4. Security of cables / electrical fittings shall be ensured
5. Systems for fire detection / suppression shall be established
6. Cleanliness of premises shall be ensured
7. Physical access to supporting infrastructure shall be restricted
8. Physical security of workstations / laptops shall be ensured
9. Equipment shall be maintained in such a way as to ensure its continued availability and integrity
10. Secure Disposal or re-use of equipment shall be ensured

Procedures

SN	Detailed Procedures
1.	Identification badges should be worn by the users when at work
	Each user should wear an identification badge to gain access to the branch/office premises. The badge must have a photo of the employee and must indicate his employee-id



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपेटिट शेड्युलड बँक)

SN	Detailed Procedures
2.	Temporary Identity Badges <ul style="list-style-type: none">Employees who have forgotten their identification badge must obtain a temporary badge by providing appropriate identification. Such a temporary badge should be valid for a single day only.Identification badges that have been lost or stolen or are suspected of being lost or stolen must be reported to the Admin Department immediately.
3.	Controls over visitor entry <ul style="list-style-type: none">All visitors must sign in at the security point/reception in a Visitors Log that is retained and reviewed by the Administration ManagerAll visitors must wear a visitor's badge when on the premises of The Bank
4.	Cables / Electrical fittings <ul style="list-style-type: none">Cables connecting computing equipment and other support equipment must be neatly organized.All electrical wiring and LAN / data cabling must be structured / concealed cabling, with the appropriate distance between both.Circuit breakers of appropriate capacity must be installed to protect the hardware against a sustained increase in power.Electrical mains must be properly guarded against accidental / unauthorized access.
5.	Fire detection and suppression <ul style="list-style-type: none">Smoking should be prohibited within the office premises.Smoke detectors must be placed at strategic locations to set off an alarm in case of fire.Fire extinguishers (which are human-friendly and usable over computer hardware) must be installed to minimize damage. In case of fire, activation of the extinguisher should be a manual process.The fire alarm, smoke detectors and extinguisher system must be inspected and tested once in six months.Training should be given to all staff members on the use of the fire extinguisher system once a year.
6.	Cleanliness of premises <ul style="list-style-type: none">The floor, walls and IT equipment must be regularly cleaned.



SN	Detailed Procedures
	<ul style="list-style-type: none">Users must ensure that their desks are clean (no confidential information should be kept in the open)
7.	Controls over supporting infrastructure
	<p>Access to facilities that support information processing systems, such as telecommunication equipment, emergency power equipment (UPS, etc.), network hubs etc. should be controlled.</p> <ul style="list-style-type: none">An adequate number of uninterrupted power supply (UPS) systems must be installed for all critical computing and supporting equipment. The UPS must have the capability to continue the power supply to allow for an orderly shutdown of the system.In areas susceptible to outages of power for more than 15 to 30 minutes per day, generators should be provided to ensure the working of the business-critical workstations.Backup power facilities must be tested at least once a month to ensure the reliable functioning of the equipment.Emergency lighting may be provided for use during power outages.CCTV cameras should be installed in such a manner that they can be easily reached by an intruder.
8.	Physical security of workstations / laptops
	<ul style="list-style-type: none">A complete and up-to-date inventory of the workstations / laptops should be maintained. Each workstation / laptop should be identified with the asset code for easy identification.Workstations / Laptops must be traceable to individual users. Each individual must be made accountable for the physical security of Workstations / laptops.All laptops must be physically secured in a locked room or cabinet whenever they are not in use.When an incident of theft of a Workstation / laptop comes to light it must be reported by the user to the Department Head, & IT Manager and the physical security department immediately.
9.	Maintenance of equipment
	<ul style="list-style-type: none">All information systems equipment must have a unique identifier/equipment code attached to it so that physical inventories can be effectively updated.Equipment should be maintained in such a way as to ensure its continued availability and integrity. The following guidelines should be considered:



SN	Detailed Procedures
	<ul style="list-style-type: none">Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications.Only authorized maintenance personnel should carry out repairs and service maintenance.Appropriate controls should be taken when sending equipment off the premises for maintenance. All requirements imposed by insurance policies should be complied with.Only authorised users should be allowed to take the equipment off premisesAppropriate record of the movement of such equipment should be maintained for tracking purposes
10.	Secure Disposal or re-use of equipment
	<ul style="list-style-type: none">Devices containing sensitive information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.In case of damaged devices, the IT department should take adequate precautions before sending the device for repair like ensuring that the vendor has executed an NDA or getting the repair done on-site rather than off-site.

Responsibilities

- General Administration department
- IT support team
- ESDS support team

xxxxxx End of Policy Documents xxxxxx

॥ सहकारेण जनकल्याणम् ॥



15. Business Continuity Management Policy

Objective

After migration to the ESDS data center facility, the responsibility of ensuring the availability of various Information Assets rests with the ESDS. ESDS is expected to provide all requirements for Bank's Business continuity.

Scope

This policy covers CBS and supports the critical business activities of The Bank. ESDS is expected to ensure the availability of the Information Assets.

Policy Statement(s)

1. A business continuity team should be established.
2. The composition of the business continuity team should be decided.
3. A comprehensive inventory of the various business processes and the associated information assets should be prepared.
4. Critical assets and supporting assets should be classified.
5. Recovery time and recovery architecture for each asset should be decided.
6. Procedures should be established for implementing BCP.
7. Procedures should be established for testing the BCP.
8. Procedures should be established for change management.
9. Contact numbers of BC team members should be maintained.
10. Procedures should be established for documentation requirements.
11. Appropriate access controls should be implemented over the soft and hard copies of the BC plan.
12. The Business Continuity Management Process and the Business Continuity Plan should be audited.

Procedures

SN	Procedures
1.	Coordinator from The Bank End
	The Bank should identify a senior management user to ensure proper coordination between The Bank and ESDS to bring up the business operations in case of a disruption.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेट शेड्युलड बँक)

SN	Procedures
2.	Composition of Business Continuity Team The Bank should constitute a BC Team headed by the above-mentioned coordinator. The BC Team should be drawn from various functions and departments and the IT manager of The Bank.
3.	Inventory of Processes ESDS should prepare a comprehensive inventory of the various business processes and the associated information assets (like operating systems, databases, application systems, network components etc.) and other resources required for business continuity. In case the production site at Nashik is not available, then ESDS should migrate to their DR site as per the terms and conditions mentioned in the SLA.
4.	Defining Recovery Time & Recovery Architecture for each asset ESDS should ensure that the business continuity is established as per the terms mentioned in the SLA e.g. ESDS should make the infrastructure available to The Bank within the parameters for Recovery Time Objective (RTO) and the loss of data / Recovery Time Objective (RTO) defined in the agreement.
5.	Testing of the BCP ESDS should ensure that The Bank's set is tested for recovery (business continuity) and that a record is maintained and submitted to The Bank for monitoring purposes.
6.	Maintaining contact numbers of BC Team members The Bank should maintain a comprehensive and up-to-date list of names, phone numbers, addresses, and contact details of the ESDS management users that is available to the BC Team.
7.	Auditing BC Plan The Business Continuity Management Process and the Business Continuity Plan should be audited to ensure that it meets the guidelines prescribed by the regulatory authorities.

Responsibilities

- Bank's BC Team

xxxxxxx End of Policy Documents xxxxxxx



16. Asset Management Policy

Objective

The purpose of this policy is to define the parameters for proper management of assets owned by The Bank. These guidelines are defined to ensure streamlining of asset procurement, maintenance and disposal. Inappropriate procurement/installation exposes The Bank to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy covers all information assets supporting the business activities of The Bank and is applicable to all users including employees, contractors, consultants and temporary users.

Policy Statement(s)

1. All the IT Assets and Services should be procured as per approved procedures in effect.
2. An up-to-date information asset register should be maintained.
3. All information assets should be tagged/labelled appropriately.
4. Proper utilization of IT Assets and Services should be ensured.
5. All the IT Assets should be properly maintained and appropriate records of IT Services should be kept up-to-date.
6. IT Assets should be adequately protected as per business and other requirements.
7. Proper security of IT Assets should be ensured.
8. Movement of IT Assets should be properly tracked and up-to-date records should be maintained.
9. Procedures should be established for the retirement of Information Assets.
10. IT Assets should be disposed of in a secure manner.

Procedures

SN	Procedures
1.	Information Asset Procurement
	All information assets should be procured after receiving a proper requisition in writing from the respective department heads. The requisitions received should be discussed in the next management meeting and if found to be in order, an appropriate procurement process should be initiated. If required, the management



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेड्युलड बँक)

SN	Procedures
	may decide to seek further details/clarifications from the concerned department head. Where necessary, multiple quotations would be sought and comparison/negotiations would be carried out before placing the order for procurement.
2.	Information Asset Inventory
	An up-to-date information asset inventory should be maintained by The Bank. A separate inventory should be maintained for those assets which are under custody / are installed at ESDS – Nashik. In the inventory register, various details like Asset Owner, Asset Custodian, Location of the asset, Risk Owner, CIA (Confidentiality, Integrity, Availability) values etc. should be entered.
3.	Information Asset Identification
	Where required, the information assets should be labelled with asset code stickers for easy identification.
4.	Information Asset Utilisation
	<ul style="list-style-type: none">• All the information assets should be used by users authorised by AUCB for discharging their official duties.• In case any user notices that an information asset is being under-utilised or is underperforming, he/she should immediately notify the CISO / IT Manager who should initiate appropriate actions.• Any changes/modifications to settings/configuration of information assets should be carried out by authorised and qualified personnel only.
5.	Information Asset Maintenance
	<ul style="list-style-type: none">• All the information assets should be maintained as per the recommendations of the respective Original Equipment Manufacturer (OEM).• Efficient strategies should be implemented by respective asset owners for the maintenance of information assets.• Where required, the respective asset owners in consultation with technical support should prepare a plan for maintenance along with operational instructions for information assets.• Appropriate records of information assets maintenance should be kept.
6.	Insurance of IT Assets
	The Bank should ensure that the IT Assets are adequately insured against the relevant threats. A record of such insurance policies should be maintained.



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेअरहुल्ड बँक)

SN	Procedures
	If ESDS is not expected to cover Bank's assets under their custody, then those assets at ESDS should also be covered under insurance by The Bank. This is dependent upon the clauses of the contract / SLA with ESDS.
7.	Information Asset Security
	<p>Though asset owners are primarily responsible for the security of their respective information assets, it is also the responsibility of all the users to ensure that the information assets being handled by them are safeguarded against damage, misuse, theft, etc. Further, no information asset should be removed from the premises without appropriate authorisation.</p> <p>"End of Support" (EOS) dates for IT Systems and Software should be closely monitored to ensure that information assets are not exposed to security risks due to the unavailability of security patches/spares from the Original Equipment Manufacturer (OEM). These risks should be documented in the Risk Assessment Register.</p>
8.	Information Asset Movement
	<ul style="list-style-type: none">• When any information asset of the organization is in transit, then the person carrying the same should be responsible for its security.• Reliable transport or a courier agency should be used. A list of authorized couriers should be agreed and the procedure to check the identification of the couriers should be implemented.• Packaging should be adequate to protect the contents from any physical damage.• Record of all in-transit information assets should be maintained.
9.	Retirement of Information Assets
	<ul style="list-style-type: none">• The Management understands that each information asset has a functional life and needs replacement at the end of its functional life. However, generally, the information asset may be replaced only when such an old asset becomes a hindrance/burden due to performance issues in day-to-day activities.• Whenever a user faces performance issues with the information asset, he/she should inform the IT Department which will perform the necessary diagnostics on the information asset.• If the information asset is deemed to be "Beyond Repair", the IT Department should inform the Head of the Department of the concerned user as well as the procurement team that the information asset needs to be replaced.• Once the information asset is replaced, the IT Department should remove the old information asset and start the disposal process.



SN	Procedures
10.	Disposal of Information Assets
	<ul style="list-style-type: none">All the information assets should be disposed of securely and safely when no longer required.In the case of records like paper documents, the same should be destroyed using a paper shredder after the prescribed period of timeIn case of permanent disposal of equipment containing the information should be irreversibly deleted before the equipment is moved off the site.A separate Disposal of IT Asset Policy (AU-IT-POL-L2-002) was created as per the recommendation in the external IS Audit for the year 2021-22; which can be referred to for more details.

Responsibilities

- Information Asset owners
- Information Asset Custodians
- IT Support Team
- ESDS Support Team
- All users

xxxxxx End of Policy Documents xxxxxx

॥ सहकारेण जनकल्याणम् ॥



17. Information Security Assurance Policy

Objectives

The purpose of this policy is to ensure that assurance of information security can be provided with the help of periodic reviews and audits.

Scope

This policy covers all information assets supporting the business activities of The Bank and is applicable to all users including employees, contractors, consultants and temporary users.

Policy Statement(s)

1. Procedures should be established for periodic review of established policies and procedures
2. Procedures should be established for carrying out system audits, and VA-PTs.
3. Rectification of observations raised in audits and VA-PT
4. Periodic review of the implementation of policies and procedures
5. Approval for non-implementation of policies
6. Ensuring compliance with the new guidelines

Procedures

SN	Procedures
1.	Periodic Review of Policies & Procedures The policies and procedures should be reviewed on a periodic basis. The period of review should not exceed one calendar year. The review should be undertaken considering various suggestions recommended through system audits as well as new guidelines/circulars released by the respective regulatory bodies.
2.	Carrying out system audits, and VA-PTs. System Audit: The main objective of the system audit will be to review the configurations of various Information Assets for policy compliance including a review of controls over physical and environmental assets. It is encouraged to use the services of outside experts.



SN	Procedures
	<p>The Bank should undertake a comprehensive system audit of all infrastructure at least once every year.</p> <p>VA-PTs (Vulnerability Analysis & Penetration Testing)</p> <p>The main objective of VA-PT will be to identify technical vulnerabilities from inside and outside The Bank's network. It is recommended to use the services of outside experts for this purpose.</p> <p>The Bank should undertake VA of critical applications and public-facing applications every 6 months while the PT should be undertaken once every year.</p>
3.	Rectification of observations raised in audits and VA-PT
	<p>The Bank should ensure that the observations raised in the audits and VA-PT are rectified within a reasonable time frame.</p>
4.	Periodic review of the implementation of policies and procedures
	<p>The Bank should undertake periodic reviews of the implementation of established policies and procedures with the help of various MIS reports and continuous monitoring.</p>
5.	Approval for Non-implementation of policies
	<p>In the case where any Security Policies cannot be implemented or are non-implementable, then approval should be obtained from the management for such non-implementation or non-rectification. A record should be maintained for such exceptions.</p>
6.	Ensuring compliance with the new guidelines
	<p>In case of any new guidelines issued by RBI or by any other regulatory or governmental bodies, suitable changes and upgrades should be made to the Security Policies.</p>

Responsibilities

- Chief Executive Officer (CEO)
- Chief Information Security Officer (CISO)
- Management and Executive Members
- IT Team
- ESDS Support Team
- All users

➤ **xxxxxxx End of Policy Documents xxxxxx**



18. Information Security Awareness Policy

Objectives

The purpose of this policy establishes the Information Security Awareness Training Policy for The Bank. This policy ensures security awareness and training controls that protect the confidentiality, integrity, and availability of The Bank's Information Resources.

Scope

The policy applies to all employees, contractors, and other stakeholders who access, use or manage information assets owned or controlled by The Bank.

Policy Statement(s)

1. The Bank shall consider security awareness as the basic component of its education strategy which tries to change the attitude, behaviour and practice of its target audience (e.g. customers, the general public, employees etc.).
2. Awareness activities shall be done on an ongoing basis, using a variety of delivery methods which shall focus on security aspects
3. Training will be provided during orientation sessions for the employees who must complete information security awareness training upon hire and thereafter.
4. Participate in mandatory regulatory and compliance-related security awareness training conducted by regulatory authorities such as the Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), and other relevant regulatory bodies.
5. To generate a standard understanding of the evolving fraud scenarios, The Bank intends to run awareness programs targeting the larger customer base.
6. To bank shall also run awareness programs for various other stakeholders, including bank employees, who can then act as resource persons for customer queries, law enforcement personnel for more understanding response to customer complaints and media for dissemination of accurate and timely information.
7. The IT and HR departments shall communicate the training schedule to employees and ensure that they complete the training in a timely manner and that training records are maintained.



Procedures

SN	Procedures
1.	Approach to awareness programs
	<p>The Bank shall follow the below three stages for developing the continual awareness program cycle:</p> <ul style="list-style-type: none">➤ Planning and design➤ Execution and Management➤ Evaluation and course correction
2.	Planning and design
	<p>The Annual Information Security Awareness Training program calendar be created.</p> <p>The program will include annual training and/or refresher courses targeting various groups of bank stakeholders.</p> <p>The Bank shall ensure that the content of the awareness programs is in the interest of its users and is relevant to their banking needs. In the planning and design stage, The Bank shall:</p> <ul style="list-style-type: none">• Establish a working group• Define goals and objectives• Define target group• Identify the needs of the target audience• Identify human and material resources required• Evaluate potential solutions• Select desired solutions and procedures• Obtain the organizational buy-in• Identify program benefits and obtain budgetary sanctions• Establish the priorities.• Prepare a work plan and checklists along with the resource requirements, timelines and milestones• Define communication framework• Define indicators to measure the progress• Establish a baseline for evaluation• Document learning• Periodic review of the work plan as the program progresses.
3.	Execution and Management
	<p>The Bank shall focus on the following activities to implement the awareness program. In the execution and management stage, The Bank shall</p>



SN	Procedures
	<ul style="list-style-type: none">Nominate team membersReview work planEngage a suitable vendor for content creation and publication.Launch and implement the activitiesDocument learning
4.	Evaluation and course correction
	<p>The Bank shall design and implement a well-calibrated feedback strategy for determining the effectiveness of the awareness program and ensuring continuous improvement. In the evaluation and course correction stage, The Bank shall</p> <ul style="list-style-type: none">Gather dataCollect feedback on communicationsAssess effectiveness through a number of eventsReview program objectivesMake necessary changes in the plan
5.	Identify Target audience
	<p>The Bank shall identify and segment the target users and customize the awareness program for the specific target groups.</p> <p>The target groups for these programs shall include:</p> <ul style="list-style-type: none">Bank customersBank employees and consultantsLaw enforcement agencies – Police, Judiciary and Consumer ForumsFraud risk professionalsMedia personnelChannel partners and suppliersGeneral public of varying age and technical knowledge – children, youth, adults, senior citizens and silver surfers
6.	Communication framework
	<p>As communication is crucial for the success of the awareness program, The Bank shall consider the following key elements for its effective communication:</p> <ul style="list-style-type: none">Ability to reach out to a broad audience thereby maximizing the reach of the messageNot to be alarming or overly negative about a situation. If issues or risks need to be detailed, real-world experiences shall be used to create a better understanding among the audience.Deliver the right message content to the right audience using the most effective communication channels



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेड्युलड बँक)

SN	Procedures
	<ul style="list-style-type: none">The message shall state the risks and threats facing the users, why it is relevant to them, what to do and not to do, and finally how to be protectedThe message shall be compelling and clearly state why security is important. Users who understand why certain types of behaviour are risky are most likely to take ownership of the issue and change their behaviour.
7.	Communication content
	<ul style="list-style-type: none">The Bank's communications shall carry information related to various frauds in general with a specific focus on electronic frauds through fake websites, phishing, vishing, skimming and emails.The Bank shall sensitize customers on the need to protect PINs, security tokens, personal details and other confidential data.Customers shall be made aware of the security practices to be followed while using electronic channels such as ATMs, internet banking and mobile banking.When new operating features or functions, particularly those relating to security, integrity and authentication, are being introduced, The Bank shall ensure that the customers have sufficient instruction and information to be able to properly utilize them
8.	Communication collaterals
	<p>The Bank shall create awareness building collaterals in the form of:</p> <ul style="list-style-type: none">Leaflets and brochuresEducational material in account opening kitsSafety tips in cheque books, PINs, account statements and envelopesReceipts dispensed by ATMsDVDs with animated case studies and videosScreensaversElectronic newslettersShort Messaging Service (SMS) textsRecorded messages that may be played during the waiting period of phone banking calls <p>The Bank shall create the collaterals in regional languages wherever required.</p>
9.	Communication Channels
	<p>The Bank shall establish more than one communication channel and use them to engage its customers successfully.</p> <p>The Bank shall use any of the below channels:</p> <ul style="list-style-type: none">Advertising campaigns through print and TV mediaTalk shows on television/radioCustomer meets and interactive sessions with specialists



दि अकोला अर्बन को-ऑपरेटिव बँक लि; अकोला

(मल्टिपट्टेड शेअरहुल्ड बँक)

SN	Procedures
	<ul style="list-style-type: none">• Common website developed with content from all stakeholders• Online training modules and demos hosted on the website• Groups, games and profiles on social media• Advertisements on online shopping sites• Bill boards• Posters in prominent locations such as petrol pumps and popular restaurants• Interactive guidance in the form of help lines• Desktops screens, Emails and SMS texts• Distance learning programs and demos <p>The Bank shall ensure that the message delivered, the channels used and the sender of the message are influential and credible.</p> <p>The Bank shall use multipliers that can help communicate to a broad range of audience, including, but not limited to:</p> <ul style="list-style-type: none">• Community centres• Schools and colleges• Computer and book stores• Libraries• NGOs• Social Clubs• Education centres• Social networking sites
10.	Research and analysis
	<p>The Bank shall form a research group to continually update the team with the latest trends and evolving modus operandi.</p> <p>The group shall maintain a repository of material such as:</p> <ul style="list-style-type: none">• Case studies• Sample mails• Sample of fraudulent documents• Data collected from victims or targets of fraud• International practices and developments
11.	Evaluation
	<p>The Bank shall evaluate the effects of various campaigns for specific target groups through qualitative (e.g. focus groups, interviews) and/or quantitative (e.g. questionnaires, omnibus surveys) methods.</p>



SN	Procedures
	The Bank shall also conduct an evaluation against metrics, performance objectives, etc. to check the campaign's effectiveness and to establish lessons learned to improve future initiatives.

Responsibilities

- Chief Information Security Officer (CISO)
- Management and Executive Members
- IT and HR Team
- All users

xxxxxx End of Documents xxxxxx

॥ सहकारेण जनकल्याणम् ॥



19. Cryptographic Key Management Policy

Objectives

The purpose of this policy is to ensure the appropriate use of cryptographic controls to protect sensitive information, especially during transfer to mobile devices or storage media. The policy also defines key management practices, including key creation, protection, distribution, storage, recovery, and destruction.

Scope

This policy applies to all cryptographic controls and key management activities associated with information assets supporting the business activities of The Bank. It is applicable to all users, including employees, contractors, consultants, and temporary users who handle sensitive information.

Policy Statement(s)

1. Cryptographic techniques must be used to protect sensitive data during storage and transmission.
2. A robust key management process must be established, covering key generation, distribution, storage, rotation, recovery, and destruction.
3. All cryptographic solutions and protocols must comply with industry standards and regulatory requirements.
4. Cryptographic keys must be protected against unauthorized access, modification, loss, or destruction.
5. Periodic reviews and audits of cryptographic controls and key management practices must be conducted.
6. Exceptions to the use of cryptography must be formally documented and approved by management.



Procedures

SN	Procedures
1.	Cryptographic Key Generation
	All cryptographic keys must be generated using approved algorithms and key lengths as per industry best practices (e.g., AES-256, RSA-2048). The generation process should ensure randomness and unpredictability.
2.	Key Protection and Storage Keys
	Keys must be stored in secure environments, such as Hardware Security Modules (HSMs) or encrypted key stores. Access to keys must be limited to authorized personnel and protected using multi-factor authentication (MFA) where applicable.
3.	Key Distribution
	Key distribution must occur over secure channels (e.g., TLS, VPN). Public keys can be distributed openly, but private keys must remain confidential and secure during transfer.
4.	Key Rotation and Expiry
	Cryptographic keys must have a defined lifespan. Keys should be rotated periodically based on sensitivity and usage. Compromised keys must be revoked immediately, and new keys generated.
5.	Key Backup and Recovery
	Key backups must be encrypted and stored securely. Key recovery processes must ensure that only authorized personnel can retrieve keys in the event of data loss or disaster recovery situations.
6.	Key Destruction
	When keys are no longer required, they must be securely destroyed to prevent unauthorized recovery. This process should follow industry-standard methods such as cryptographic erasure.
7.	Audit and Review
	Regular audits must be performed to ensure adherence to cryptographic policies and key management practices. Any anomalies or weaknesses identified must be promptly rectified.
8.	Exception Management
	Any exceptions to this policy must be documented with justification and approved by the management team. Records of such exceptions must be maintained for audit purposes.



Responsibilities

- **Chief Information Security Officer (CISO):** Oversight of cryptographic controls and key management processes.
- **IT Security Team:** Implementation and maintenance of cryptographic techniques and key management procedures.
- **IT Team:** Day-to-day management and protection of cryptographic keys.
- **All Users:** Compliance with cryptographic policies when handling sensitive data.

xxxxxx End of Documents xxxxxx

॥ सहकारेण जनकल्याणम् ॥



20. Teleworking Policy

Objectives

The purpose of this policy is to ensure that teleworking is undertaken safely from an information security perspective. It aims to identify, assess, and manage information security risks associated with teleworking to protect organizational data and resources.

Scope

This policy applies to all teleworkers who use organizational computing resources or their own resources to connect to organizational facilities. It is applicable to all employees, contractors, consultants, and temporary users engaged in teleworking activities.

Policy Statement(s)

1. Authorization for teleworking must be granted only if the organization provides suitable teleworking facilities, such as equipment, access to the organizational network, and necessary software.
2. An information security risk assessment must be conducted before approving teleworking, considering factors such as the criticality of the accessed information, confidentiality requirements, and teleworking technology suitability.
3. Teleworking equipment and solutions must be fully supported, maintained, and returned securely upon termination of the arrangement.
4. Teleworkers must follow proper security protocols, including data backup, use of licensed software, and compliance with secure remote access mechanisms approved by IT Services.
5. Confidential information must be adequately protected, requiring full-disk encryption for teleworking computers and secure handling of hardcopy documents.
6. Teleworking access must be monitored, and vendor remote access IDs should be enabled only when needed and disabled afterward.
7. Violations of this policy must be reported to the Information Security Head, and non-compliance may result in disciplinary actions or withdrawal of access.



Procedures

SN	Procedures
1	Teleworking Authorization
	Approval for teleworking must follow an assessment process that evaluates security risks and requires authorization from the department head.
2	Provision of Teleworking Equipment
	IT Services must provide, support, and ensure proper documentation on the usage of teleworking equipment. Upon termination, all devices and data must be returned securely.
3	Secure Remote Access
	Remote access solutions must be configured with strong authentication methods (e.g., two-factor authentication) and approved by IT Services before deployment.
4	Information Security Compliance
	Teleworkers must follow security protocols such as encrypted connections, firewalls, and anti-malware solutions to protect organizational data.
5	Data Backup and Protection
	All teleworking solutions must support adequate data backup procedures. Employees must understand and follow these backup guidelines to prevent data loss.
6	Secure Handling of Confidential Documents
	Confidential data should be accessed remotely rather than stored locally. If physical documents are needed, they must be kept in locked cabinets and disposed of securely (e.g., shredding).
7	Monitoring and Access Control
	IT Services must monitor teleworking access and ensure remote access accounts are disabled when no longer required. Vendor access must be temporary and monitored when in use.
8	Policy Violations and Exceptions
	Any deviations from this policy must be documented, justified, and approved by management. All exceptions must be recorded for audit purposes.



Responsibilities

- **Chief Information Security Officer (CISO):** Oversight of teleworking security measures and compliance monitoring.
- **IT Security Team:** Implementation and enforcement of security controls related to teleworking.
- **IT Team:** Provision, support, and management of teleworking equipment and secure remote access.
- **All Teleworkers:** Adherence to teleworking security protocols, secure handling of data, and compliance with this policy.

This policy is subject to periodic review and updates to ensure alignment with security best practices and organizational needs.

xxxxxx End of Policy Documents xxxxxx

॥ सहकारेण जनकल्याणम् ॥



दि अकोला अर्बन को-ऑपरेटिव बैंक लि; अकोला

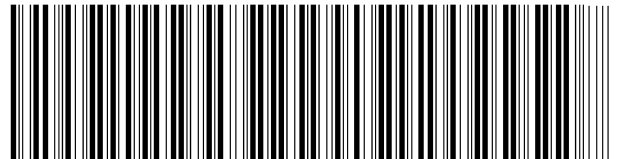
(मल्टिपट्टेड शोल्डरड बैंक)

COPYRIGHT NOTICE

Copyright © by
The Akola Urban Co-operative Bank Ltd., Akola

*All Rights Reserved. The contents of this document are confidential and proprietary to The Akola Urban Co-operative Bank Ltd., Akola and no part of this document should be reproduced, published in any form by any means, electronic or mechanical including photocopy or information storage or retrieval system nor should the material or any part thereof be disclosed to third parties without the express written authorization of The Akola Urban Co-operative Bank Ltd., Akola. Access to and use of this document shall refer to The Akola Urban Co-operative Bank Ltd., Akola's **Information Classification and Control Policy**.*

॥ सहकारेण जनकल्याणम् ॥



AU - I SMS - POL - L1 - 003