Information Technology & Information Security Policy

THE KEONJHAR CENTRAL CO-OPERATIVE BANK LTD.
KEONJHAR Tel. 06766-255183, 253137
Fax-253137

Sl No	TOPICS	Page No
	INFORMATION TECHNOLOGY POLICY	
PART-I A		1 - 10
1.	Introduction	1
2.	Information Technology and Changing Face of Banking	1
3.	IT is one of the Major Drivers of Banking Business	2
4.	Yet "IT" can cause Business Vulnerability	2
5.	Information Security (IS) Defined	3
6.	Our Bank and IT	4
7.	IT Security and Controls in the Bank	4
8.	Information Security Policy: Objectives 8.1. The Policy.	4
9.	Scope of the IS Policy	5
10.	Owners and Custodians	5
11.	Responsibility	5
12.	Steering Committee/ Information Security Committee	6
13.	Chief Information Security Officer (CISO)	6
14.	Business Heads	7
15.	Coverage of the Policy	7
16.	To Achieve the Objectives	7
17.	IS Review	8
18.	Applicability and Exceptions	8
19.	Box: Certain Terms Explained	9
PART-I B		11-18
1.	Information Systems Security Policy	11
2.	**Environment & Physical Security** Purpose Policy Statement	11 11 11
3.	**Acceptable Usage Security** Purpose Policy Statements	11 11 12
4.	**Incident Management** Purpose Policy Statement	12 12 12
5.	**Asset Classification & Handling**	12
	Purpose Policy Statement(ISO 27001(ISMS)) NIST Cyber security Framework CSA framework & ISO 27701(PIMS)	12 12 12 12

SL. NO.	TOPICS	PAGE NO.
6.	**Asset-Media Disposal**	13
	Purpose	13
	Policy Statement	13
7.	**Anti- Virus**	13
	Purpose	13
	Policy Statement	13
8.	**Networking & Internet Security**	13
	Purpose	13
	Policy Statement	14
9.	**Operating Systems**	14
	Purpose	14
	Policy Statement	14
10	**Applications**	14
	Purpose	14
	Policy Statement	14
11.	**Database**	15
	Purpose	15
	Policy Statement	15
12.	**Patch Management**	15
	Purpose	15
	Policy Statement	15
13.	**Back-up**	15
	Purpose	15
	Policy Statement	15
14.	**Personnel**	16
	Purpose	16
	Policy Statement	16
15.	**Password**	16
	Purpose	16
	Policy Statement	16
16.	**E-mail Usage and Security**	16
	Purpose	16
	Policy Statement	17
17.	**Change Management**	17
	Purpose	17
	Policy Statement	17
18.	**Monitoring**	17
	Purpose	17
	Policy Statement	17
19.	**Outsourcing/Third Party**	17
	Purpose	17
	Policy Statement	18

SL. NO.	TOPICS	PAGE NO.
20.	**Business Continuity**	18
	20.1 Purpose	18
	20.2 Policy Statement	18
21.	**ATM Security Policy**	18
	21.1 Purpose	18
	21.2 Policy Statement	18
PART II – INFORMATION SYSTEMS SECURITY POLICY		19-67
	Policies and Procedures	19
2.	**Environment and Physical Security Policy**	19
	2.1 Purpose	19
	2.2 Policy Statement	19
	2.3 Procedures: Scope	19
	2.4 Access Control	19
	2.5 Environmental Protection	20
	2.6 Data Centre Security	20
	2.7 Identification of Devices	20
	2.8 CCTV Monitoring	20
	2.9 Power at the Data Centre	20
	2.10 Fire Prevention and Control	21
	2.11 Environmental Safeguards	21
	2.12 Preventive Maintenance	21
	2.13 Monitoring	21
	2.14 Document Security	21
	2.15 Enforcement	22
3.	**Acceptable Usage Security**	22
	3.1 Purpose	22
	3.2 Policy Statement	22
	3.3 Scope	22
	3.4 Desktop Users	22
	3.5 Laptop Users	23
	3.6 Password Security	24
	3.7 Internet Usage	25
	3.8. Clear Desk	25
4.	**Incident Management**	25
	4.1. Purpose	26
	4.2. Policy Statement	26
	4.3 Scope	26
	4.4 Incident Identification	26
	4.5 Incident Reporting	26
	4.6. Incident Verification	27
	4.7 Incident Recovery	27
	4.8 Incident Prevention	27

SL. NO.	TOPICS	PAGE NO
5.	**Asset Classification & Handling**	27
	5.1 Purpose	27
	5.2 Policy Statement	28
	5.3 Procedure for Asset Classification and Handling: Scope	28
	5.4 Accountability	28
	5.5 Information Classification	28
	5.6 Document Classification	29
	5.7. Secret Documents	29
	5.8. Confidential Documents	29
	5.9 General Documents	29
	5.10 Media Handling	29
	5.11 Enforcement	29
6.	**Asset-Media disposal**	29
	6.1 Purpose	29
	6.2 Policy Statement	29
	6.3 Scope	30
	6.4 Disposal of Information Assets	30
	6.5 Disposal of Electronic Media	30
	6.6 Disposal of Paper Based Media	30
	6.7 Condition for Disposal of IT Assets	31
	6.8 Disposal of IT Asset - Procedure	31
	6.9 Periodicity of Disposal of Obsolete IT Assets	31
	6.10 Outsourcing of Disposal of IT Assets	31
	6.11 Enforcement	32
7.	**Anti- Virus**	32
	7.1 Purpose	32
	7.2 Policy Statement	32
	7.3. Scope	32
	7.4 Installation	32
	7.5 Anti-Virus Support Team	33
	7.6 Anti-Virus Signature Update	33
	7.7 Status Reports	33
	7.8 Server Security	33
	7.9 Server Monitoring	33
	7.10 Tracking New Vulnerabilities	34
	7.11 Documentation	34
	7.12 External Users	34
	7.13 Backup and Redundancy	34
	7.14 Reporting	34
8.	**Networking & Internet Security**	34
	8.1 Purpose	34
	8.2 Policy Statement	35
	8.3 Scope	35
	8.4 Internet Access	35
	8.5 Dial out Access	35

SL. NO.	TOPICS	PAGE NO.
	8.6 WAN access on bank's network	35
	8.7 Segregating Server and User Segments	36
	8.8 External Access	36
	8.9 Dial in Access	36
	8.10 Redundancy	36
	8.11 Network Device Configuration	36
	8.12 Documentation	36
9	**Operating Systems**	37
	9.1 Purpose	37
	9.2 Policy Statement	37
	9.3 Scope	37
	9.4 User Authentication	37
	9.5 Account Policy	37
	9.6 New User Provisioning	37
	9.7 Security of User Credentials	37
	9.8 Logging	38
	9.9 Non-Essential Services	38
	9.10 Login Banner	38
	9.11 Anti-Virus	38
	9.12 Naming Conventions	38
	9.13 Documentation	38
	9.14 Review of User Access Rights	38
	9.15 Emergency Procedures	38
10.	**Procedures for Application Security**	38
	10.1 Purpose	38
	10.2 Policy Statement	39
	10.3 Scope	39
	10.4 Application Owner	39
	10.5 Application Access	39
	10.6 Data Security	40
	10.7 Input Controls	40
	10.8 Processing Controls	40
	10.9 Account Policy	40
	10.10 Database Access	40
	10.11 Audit Trails	40
	10.12 Error Handling	41
	10.13 Capacity Planning	41
	10.14 Performance Testing	41
	10.15 Security Testing	41
	10.16 Documentation	41
11.	**Database**	41
	11.1 Purpose	41
	11.2 Policy Statement	41
	11.3 File System Security	42
	11.4 User Authentication	42

SL. NO.	TOPICS	PAGE NO.
	11.5 New User Provisioning	42
	11.6 Account Policy	42
12.	**Patch Management**	43
	12.1 Purpose	43
	12.2 Policy Statement	43
	12.3 Scope	43
	12.4 Identification & Validation of Patches	43
	12.5 Patch Classification	44
	12.6 Patch Scheduling & Prioritization	44
	12.7 Patch Application Procedure	45
	12.8 Patch Tracking	45
	12.9 Audit & Assessment	45
	12.10 Centralized Patch Management System	45
	12.11 Enforcement	46
13.	**Back-up**	46
	13.1 Purpose	46
	13.2 Policy Statement	46
	13.3 Scope	46
	13.4 Backup Process	46
	13.5 Security of Backup Media	47
	13.6 Migration of Backup Data	47
	13.7 Recovery Testing	47
	13.8 Documentation	47
14	**Personnel**	47
	14.1 Purpose	47
	14.2 Policy Statement	47
	14.3 Scope	48
	14.4 Terms of Employment	48
	14.5 Training and Awareness	48
	14.6 Compliance	48
	14.7 Termination	49
15.	**Password**	49
	15.1 Purpose	49
	15.2 Policy Statement	49
	15.3 Scope	50
	15.4 Construction of Passwords	50
	15.5 Disabling Access	50
	15.6 Generation of Password	50
	15.7 Resetting Passwords	51
	15.8 Customer Facing Applications	51
	15.9 Resetting of Default Passwords	51
	15.10 Compliance to Password Policy	51
	15.11 Enforcement	52

SL. NO.	TOPICS	PAGE NO.
16.	**E-mail Usage and Security**	52
	16.1 Purpose	52
	16.2 Policy Statement	52
	16.3 Scope	52
	16.4 E-mail Service – General	52
	16.5 Account Protection	53
	16.6 Server Monitoring	53
	16.7 Monitoring & Reporting	53
	16.8 Document and Storage Security	53
	16.9 Backup and Redundancy	53
	16.10 Change Management	54
17.	**Change Management**	54
	17.1 Purpose	54
	17.2 Policy Statement	54
	17.3 Scope	54
	17.4 Change request and approval	55
	17.5 Testing of Implementation Plan	55
	17.6 Implementation of Change	55
	17.7 Minor/Emergency Changes	56
	17.8 Review of Change	56
18.	**Monitoring**	56
	18.1 Purpose	56
	18.2 Policy Statement	56
	18.3 Scope	56
	18.4 Security Monitoring	56
	18.5 Performance Monitoring	57
	18.6 Log Monitoring	57
19.	**Outsourcing / Third Party**	57
	19.1 Purpose	57
	19.2 Policy Statement	57
	19.3. Scope	58
	19.4 Outsourcing Plan	58
	19.5 Vendor Selection	58
	19.6 Transition Risks	58
	19.7 Security	59
	19.8 Performance	59
	19.9 Contractual Terms	59
	19.10 Conformity to RBI Guidelines	60
20.	**Business Continuity**	60
	20.1 Purpose	60
	20.2 Policy Statement	60
	20.3 Scope	60
	20.4 DR Requirement	61
	20.5 Business Impact Analysis	61

SL. NO.	TOPICS	PAGE NO.
	20.6 Disaster Recovery Strategy (DRS)	61
	20.7 Disaster Recovery (DR) Plan	61
	20.8 Awareness and Training Program	61
	20.9 Testing of DR Plan	61
	20.10 Review of DR Plan	61
	20.11 Maintenance of Emergency Contact Numbers	62
21.	**ATM**	62
	21.1 Purpose	62
	21.2 Policy	62
	21.3 Scope	63
	21.4 Physical Security	63
	21.5 General Security	63
	21.6 Issue of Personalized ATM Card & Pin Mailer	65
	21.7 Loss and Theft of Card	65
	21.8 ATM Network Security	65
	21.9 Confidentiality	66
	21.10 Data Integrity	66
	21.11 Key Management	66
	21.12 Authentication	66
	21.13 Non-Repudiation	66
	21.14 Access Control	67
	21.15 Security	67
	21.16 Audit	67
	21.17 Activity Reporting	67
	21.18 Security Recover	67
22.	**AADHAR ACT,REGULATIONS & SPECIFICATIONS**	68
	22.1 Data Encryption	68
	22.2 Limited Data storage	68
	22.3 Authentication Methods	68
	22.4 Access control	69
	22.5 Consent Mechanism	69
	22.6 Logging & Auditing	69
	22.7 Secure device Standards	69
	22.8 VID	69
	22.9 **Aadhaar (Authentication) Regulations, 2016**	69
	22.10 Aadhaar (Data Security) Regulations, 2016	69
	22.11 **Aadhaar (Sharing of Information) Regulations, 2016**	69

PART-I A

1. Introduction

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.

Customer confidentiality is important for all businesses but it is an USP for banking business and hence more important. In order to maintain customer confidentiality and cater to business growth, information has to be fully protected from a variety of threats so as to ensure confidentiality, integrity & availability. The confidentiality, integrity and availability of information in the right place to the right person for right purposes are essential for any bank of financial institution to maintain its competitive edge, cash flow, profitability, legal compliance and reputation.

The adoption of Information Technology (IT) has brought about significant changes in the way the banking and the financial institutions create, process and store data and information. The communication networks have also played an equally catalytic role in the expansion and integration of the Information Systems, within and among the banks, facilitating data accessibility to different users.

Loss of information may lead to (a) financial losses which need to be minimized and (b) loss of reputation which must be avoided. In view of this it is important that our bank puts in place an appropriate set of controls & procedures to achieve impeccable IS (IS) to ensure that data is accessible and accessed only by authorized users of data and is completely inaccessibility to all others (unauthorized persons trying to use the system, information etc.). Essentially this is an issue of data integrity and implementation of safeguards against all security threats to guarantee information and information systems security across our Bank.

As technology is evolving and ever changing it is possible that information systems in operation in banks may not have been designed to be sufficiently secure. Further, the level of security, which can be achieved through the application of technology, could be limited unless it is supported by appropriate management policies and procedures. The selection of the security controls requires careful and detailed planning. It is clear that the success of information systems security cannot be achieved except with the participation by all the employees in the Bank. It will also require support and participation from the third parties such as the suppliers, vendors, contractors and customers. This calls for our bank to define, document, communicate, implement and audit information and Information Systems Security.

2. Information Technology and Changing Face of Banking.

Over the last three decades banking industry in India has adopted Information and Communication Technology (ICT) which has resulted in a paradigm shift in the way

banking is done in the country. Over the years, what started as a Ledger Posting Machine has moved through Total Branch Automation (TBA) to today's Core Banking Solutions (CBS) and other applications supported I T driven banking. It is seen that banking technology has not only changed the way customer perceives the bank but also the way bank drives its business. Customer is more keen to use latest technology driven access to banking so that he/she is able to save time and effort in doing banking.

Continuous use of banking technology has enabled the banks to have a re-look into their business processes, reengineer the same to make them effective & efficient. Rapid technological up-gradation has increased the business volumes without having to increase the branch net-work. Simultaneously there is a demand for processing large amount of information within banks to enable better decision making in response to the changing business environment. The ability of technology to manage large volume of data and has resulted in IT moving from a support function to the main driver of banking business.

Thanks to the impact of IT, banks' are now able to offer Automated Teller Machine (ATM), Cards (both debit and credit), internet banking and mobile banking to its customers. The CBS gives the customer access to transact his/her account from any of the branches or from home or work place at any time. In the recent years as e-commerce has started flourishing. Banks have stepped in to complement the process as payment gateways for e-shopping, etc. Within the bank internal processes such as accounting, ledger maintaining and other processes within bank are no more manual but are more efficient due to IT driven processing of internal data/activities & back office operations.

3. IT is one of the Major Drivers of Banking Business

Over the years our bank has been making increased use of IT in business. Our bank has taken the following IT driven initiatives.

Implemented Core Banking System for State Cooperative Bank and all the DCCBs in 2013-14.

Implemented RTGS, CTS and DBT applications

Rupay Card Project has been implemented.

Planning to introduce new Technological initiatives like Mobile Banking, Internet Banking, etc., shortly. KCC cards are being converted into Rupay Smart Cards simultaneously with PACS Computerization.

3.2 In view of this dependency of our bank on IT is fairly high. Further, IT will be central to all transaction processing. This dependence on IT is only expected to increase with time as newer technology comes into being & keeps on creating better prospects for banking business. Eventually our entire business processes will be through the use of IT.

4. Yet IT can cause Business Vulnerability

Banking technology is the use of advances in ICT for enhancing banking business.

Use of technology can cause certain vulnerabilities due to possible external or internal attack, which may result in failure of the underlying information systems and compromise information assets. There is a risk for data loss due to malafide or accidental or unauthorized access, use, misappropriation, modification or destruction of information, information systems & IT. This possibility is accentuated as the number of users accessing information systems within and outside the bank is on the high side and will keep increasing. As such exercising effective control over the information will remain a challenge. In view of the above the use of IT in banking has necessitated a completely different set of controls & processes to maintain & monitor and ensure security effectiveness. Managing vulnerability in IS cannot be manual. It is for this reason that business houses, public services and individuals manage the gap between the traditional security and controls and demand put forth by newer technologies by relying on newer technologies. Each new technology may bring in additional concerns about security.

5. Information Security (IS) defined

IS **(IS)** is concerned with safe guarding information and data both in electronic and physical form, from unauthorized access, perusal or inspection resulting in misuse, disclosure, modification, recording and destruction. IS ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability). In its guidelines for the Security of Information Systems and Networks, OECD has brought out nine principles namely Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design & Implementation, Security Management, and Reassessment.

IS framework is a set of policies, procedures, rules, regulations, compliance and review functions ensure smooth implementation and seamless operations, to achieve the business objectives. IT is, without doubt a business driver and the risk management thereof is the area of concern for IS. The three major constituents of any I S framework/architecture are people, process & technology. First of all, since technology is continuously evolving, security has to move in tandem and keep pace with it. Our bank will ensure that IS (I S) methods are appropriate to the I T architecture. Secondly the policy has to factor in the changed processes. Our bank will evaluate every new process critically in the angle of security. Thirdly people will have to understand and implement the policy. This will be ensured by capacity building. Further our bank will adhere to RBI's and other regulatory guidelines on the issue.

Efficient IS framework is also a function of *awareness, knowledge and skills.*

IT Governance entails number of activities for Board & Senior Management becoming *aware* and impact of IT on a bank.

IT Security teams require *skills,* 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 day-to-day basis to use IT. For example for 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 statements.

6. Our Bank and IT

Our Bank is using many new technologies in the banking operations. The bank is aware of the security and other challenges faced by it which has led the bank to draft policy guidelines to ensure that its information assets are secured & controlled.

The bank's business philosophy is to ensure optimum use of technology in carrying out the business, while at the same time and under any circumstances not compromising information and data security. Further, the bank is committed to conduct its business activities in such a manner that business process are smooth, customer service is excellent and business growth is continuous.

7. IT Security and Controls in the Bank

Our bank has introduced technology in a number of areas as mentioned above. In view of this, the implementation of processes will change along with the way we do our business. The focus will shift from branch to bank. Customers will be able to access their accounts from their home. On account of these changes, certain risks are foreseen in the area of security of the bank's information assets in terms of unauthorized access to bank's information and data, breakdowns in business due to technical issues or non-availability of technology support, frauds and theft in the ATMs and card business and customers facing difficulties in accessing their accounts or customers being subject to electronic threat etc. In fact the list of vulnerable areas is large. Every one of the known vulnerability needs to be addressed if it has to be ensured that users of bank's services and banks customers have full confidence that the bank and its information systems will operate as intended without failures or problems. Bank cannot guarantee that breach of security will not happen, but it will like to minimize such possibilities. Here again bank will ensure that technology is optimally utilized and that IT enhances future growth. It is in this background that the bank is putting in place an IT security system and control mechanism to minimize the risk of security incidents involving IT usage.

8. IS Policy: Objectives

8.1 The Policy.

"This IS Policy of Keonjhar Central Co-operative Bank has been established with an objective of protecting all critical information and information processing assets in order to ensure secure and correct provision of services to its customers and ensure business continuity"

The objective of this is to ensure that the information assets of the bank are appropriately

protected against the breach of confidentiality, failures of integrity and/or interruptions to their availability. IS is concerned with various channels like spoken, written, printed, and electronic or any other medium and also with the handling of information with reference to creation, viewing, transportation, storage or destruction. The users of technology in the bank are its employees, vendors, employees of vendors and most importantly the customers. This IS Policy provides management direction and support towards IS across all relevant levels and locations within and outside the bank.

This policy mandates the IS Management at the bank. It communicates top management's commitment towards establishment and implementation of all security controls and mechanisms as given out in this and other documents lays down the structure of IS management in the bank.

9. Scope of the IS Policy

IS policy is applicable to all information assets of Keonjhar Central Cooperative Bank, those are electronically stored, processed, documented, transmitted, printed and/ or faxed. The policy applies to all employees and external parties which term includes suppliers, vendors, third party users, contract staff, outsourced service providers and consultants of the bank's Primary Data Centre, Disaster Recovery Centre/Cell, CBS, Department of IT as well as all other locations of the bank.

10. Owners and Custodians

For a policy to be effective it is imperative that each the stakeholders understand clearly his/her as well as other's roles & responsibilities within the organizational framework.

Important aspects of the role are (a) Governance, (b) Strategy, (c) Creation, implementation, operations, compliance and review of the IS policies in line with the banks broad requirements and activities.

Board of Directors of the bank is the owner of IS Policy. Chief IS Officer (hereafter referred to as CISO) will be the custodian of the policy.

11. Responsibility

Board of Directors: Board alone can make changes in the policy. The Board is vested with the overall responsibility of IS. It will develop policy guidelines to be conveyed and implemented by various layers in the organization namely people (employees and other persons entrusted with the responsibility of different business functions) at senior, middle and the grass-root levels. In doing so, the Board will keep in reckoning major objectives of the IS. IS policy should be such that people, when they are aware of the banks' expectations from them, are able to implement the policy in full and without any deficiency. In this regard;

1. Policies have to be clear and well enunciated
2. Policy should be supported with standards, guidelines & procedures
3. Policy should be statements on macro, major and organizational level issues.
4. Procedures and rules should deal with implementation of policy statements.

Implementation should cover procedure, functions and technologies

5. IS strategy has to be aligned with business objectives, indicate scope of ownership and individual and team responsibilities for the policy. These should include items such role of IT security officer, owners of information assets, custodian and users
6. Policy will also need the support of investment for enabling IS and such will deal with budgeting, financial outlay, reporting etc.
7. Policy must be reviewed in regular periodicity at least annually. The focus of the Policy review will be continuous improvement in IS
8. IS governance must comply with relevant legal and regulatory requirements

It is provided that in exceptional and emergency situations IS Committee can approve emergency changes in the Policy which should be ratified by the bank in the meeting immediately after such changes.

12. Steering Committee/ IS Committee.

The IS Committee (ISC) of the bank is responsible for implementation of security policy and for dissemination of IS Policy across all business functions. The Managing Director (MD) of the bank will be the Chairman of the Committee and the CISO will be its convener. Select Business heads of the bank will be members of the committee. The committees' main focus will be supervising and oversight of IS. It will also align & integrate IT and IS strategy with business goals. The committee will meet on a regular basis to discuss implementation of IS.

- The committee shall be responsible for making budgets, reviewing the security procedures, and compliance, as also guide people with corrective action where needed. Information Security Committee will ensure that threat &vulnerabilities are evaluated, and initiate/undertake remedial action, where ever necessary on an ongoing basis
- Risk management Committee/function of the bank will also review IT security in a routine manned and will take care for promoting security throughout the bank including assisting development of IT based measures and compliance
- Bank shall ensure that technology is available for updating in a manner that efficiency and security are given paramount importance. Best process can be defined as Corporate IS Policy (CISP) about deployment, use and maintenance for all people as per the various levels.
- Lastly audit, fraud monitoring management to review to take care of compliance

13. Chief IS Officer (CISO)

The bank will nominate/appoint a CISO or entrust the exclusive responsibility of CISO to an official of the bank by whatever name called. CISO is responsible for ensuring that IS policies are regularly updated and reflect the bank's requirement.

CISO will have a dedicated, skilled & adequate staff team. The job role of CISO will include:

1. create, maintain and disseminate IS strategy, plans policies and procedures
2. carry out assessment and review of IS risk threats and vulnerability assessment in regular periodicity,
3. monitoring & reporting on a continuous basis
4. will obtain approval at appropriate level for IS plan, budget, resources and provide on-going support activities
5. Ensure that monitoring, testing and reporting of IS is done in an on effective and efficient manner. Will install effective controls to ensure compliance with IS norms.
6. establish and maintain awareness and training to promote IS across the bank

14. Business Heads

Business heads are the officials in-charge of various offices and functions (Heads of department in the HO and branch heads). They are responsible for enforcing the implementation of IS Policy within their control or area of operation. It is however clearly stated that every bank Employee, officer and contractors/consultants must comply with IS Policy and protect the bank's information assets.

15. Coverage of the Policy

Covers all forms of electronic / print information etc. on servers, desktops, networking and communication devices, tapes, CDs, USBs and other devices. Information printed or written on paper or transmitted by facsimile or any other medium is also covered.

Envisages that appropriate procedures will be created and followed at various levels of the bank to ensure absolute protection of IS. The IS objectives are set for its continual improvement.

Provides directives towards IS within the Bank

Recommends appropriate security controls that have to be implemented to maintain and manage IS system in the bank.

16. To Achieve the above Objectives

The bank shall be establishing and organizing the IS governance framework so as to ensure alignment of the IS of the bank with business strategy to support growth and other organizational objectives.

The bank will also be developing and maintaining an effective IS management system supported by appropriate procedures and rules in consonance with the policy.

Through the CISO the bank will conduct periodic risk assessments and ensure adequate, effective and tested controls for people, processes and technology to enhance IS. Through this means the bank will ensure that critical information is

Protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional.

The bank recognizes that this will call for deploying appropriate technology and infrastructure and training its people. The bank will particularly insist on its senior officials for monitoring, reviewing, exception reporting and taking actions thereof for improving the effectiveness of the IS management system.

The bank will provide an environment for promoting 'best practices' relative to its business, information systems and infrastructure;

The bank will ensure that all legal and contractual requirements with regard to IS are met wherever applicable and that any security incidents and infringement of the Policy, actual or suspected, are reported and investigated;

The bank will organize awareness programs and training on IS to all Employees as also other stakeholders such as contractors, consultants, vendors etc.

More importantly the bank will (a) take immediate and suitable actions for managing violation(s), if any of the IS Policy; and (b) develop a IS compliance culture in the bank.

17 IS Review

The implementation of IS in the bank will be one of agenda items of all Board meeting. Further the IS Policy document shall be reviewed, by the Board periodically and at least once a year as also at the time of any major change(s) in the existing environment which will affect the policies and procedures. The reviews will cover the following:

CISO report on IS and its implementation

Impact on the risk profile in the bank due to changes in the information assets, technology/ architecture, regulatory and legal requirements. The impact assessment will focus on effectiveness of IS policies and periodic compliance review of the policy adherence.

It is possible that as a result of the reviews there could be some need to frame additional policies or amend/update the existing policies. These additions and modifications will be incorporated into this IS Policy document. Policies that are not relevant due to changes in the regulation etc. shall be withdrawn.

18. Applicability and Exceptions

All employees and external parties are required to strictly comply with IS Policy. The bank has announced that **non-compliance to IS Policy is a ground for disciplinary action.** This provision will be incorporated in the Bank's disciplinary policy.

Exceptions

The IS Policy is a guideline and a policy pronouncement on IS requirements which is needed in the business interest of the bank. However for smooth conduct of business exceptions against individual controls in specific policy domains shall be documented and formally approved by GM operations in consultation with Head IT.

19. Certain Terms Explained

1. Policy & Procedures how distinguished?

"Policies" are management instructions indicating a course of action, guiding principles, and appropriate procedure. Policies are mandatory and can also be thought of as the equivalent of an organization structure and governance giving responsibilities and segregation of duties for a given objective say protection of a bank's information and information assets. Policies are distinct from and considerably higher-level than "procedures" (sometimes called "standard operating procedures"). A policy statement describes an issue or an aspect or a subject only in a general way for addressing a specific problem. Procedures are specific operational steps or methods that employees must follow/use to achieve goals (collection of procedures in a sequence could be called as a manual). A user manual in IS will include all rules and regulations and procedures that an employee must follow in day to day operations. It will also contain a set of do's and don'ts and a FAQ as well.

A standard could define how a software has to be used to perform back-ups and how to configure that software. A procedure could describe how to use the back-up software, the timing for taking back-ups, and other ways that Users interact with the back-up system. Policies drives standards and procedures and all of them require compliance. Policies provide general instructions, while standards provide specific technical requirements. Operational steps are known as procedures.

2. Who is an Information Owner?

Data and records stored on systems are responsibility of Information Owner, like business executive, business managers, and asset owners within the organization. The owner/s may delegate ownership responsibilities to another individual, mostly personnel. While doing so the owner has to ensure that appropriate procedures are in place and followed to protect the integrity, confidentiality and security of the information used or created within his/her/their area. They can authorize access and assign custodianship of information and information asset. Specify controls and communicate the control requirements to the custodian and users of the information. Owner must promptly inform the CISO about loss or misuse of information, who will initiate appropriate actions when problems are identified. CISO has to promote education and awareness by training programs administered where appropriate.

3. Who is an Information Custodian?

The custodian of information is the person who is generally responsible for the processing and storage of the information. Responsibilities may include:

- Providing and/or recommending physical safeguards.
- Providing and/or recommending procedural safeguards.
- Administering access to information.
- Evaluating the cost effectiveness of controls.
- Coordinating the maintenance of IS policies, procedures and standards as appropriate and in consultation with the IS Officer.
- Report promptly to the IS Officer the loss or misuse of any authenticated device.
- Report promptly to the IS Officer the loss or misuse of information.
- Initiate appropriate actions when problems are identified.

4. Who are Information Users?

User of information could be any employee irrespective of the level of hierarchy and will also include contractual personal, vendors, employees of vendors, employees of service providers etc. They are expected to:

- Access information only in line with authorized job responsibilities or roles.
- Comply with IS Policies and Standards and with all controls established by the owner and custodian.
- Adhere to all norms regarding disclosures of confidential information and refer to the authority where ever the disclosures are not defined. .
- Keep authentication devices (e.g. passwords, Secure-Cards, PINs, etc.) confidential.
- Report promptly to the IS Officer the loss or misuse of any authenticated device.
- Report promptly to the IS Officer the loss or misuse of information.
- Initiate appropriate actions when problems are identified.

5. What is Outsourcing?

In keeping with this international trend, it is observed, that banks in India too have extensively outsourced various activities. Outsourcing means asking a third party to do a set of activities for the bank either outside the bank or inside the bank. These activities are not performed by the employees of the bank but by the employees of the outsourcing firm. Outsourcing could be process outsourcing or a complete vertical being managed by outside firms. Needless to say, such outsourcing, results in banks being exposed to various risks. The outsourcing activities are subject to regulatory oversight. The interests of the customers have to be protected. Typically IS is concerned with outsourced information which include operational, data processing, back office and third party related activities. The outsourcing of any activity by bank does not diminish its obligations, and those of its Board and senior management, who have the ultimate responsibility for the I S aspects as well as business aspects of outsourced activity. Banks would, therefore, be responsible for the actions of their service providers including the confidentiality of information pertaining to the customers that is available with the service provider. Banks should retain ultimate control of the outsourced activity.

PART-I B

1. Information Systems Security Policy

Comprehensive IS policy document has to be, overall, in alignment with the business management objectives. The policy statements have to be further granulated for arriving at documented procedures.

The policy statements are provided in this Part (Part – B) of the document. Chief Information Systems Security Officer (CISO) would be responsible for the implementation, review and updating of the Information Systems Security. He will be assisted by a team of Officers comprising both Technical and Banking Officers. CISO will be responsible for the implementation of information systems security policy's in each and every one of the offices/locations of the bank.

CISO in the bank will be fully involved in various issues such as the development of the Information Systems Security Policy, updating of the Information Systems Security Guidelines on an on-going basis. In performing his role the CISO will work through the existing systems and as such the banks administration department will among others, have the responsibility of the security controls and compliance with the information systems security guidelines.

2. Environment & physical security

Purpose

Control of physical and electronic access to confidential information and computing resources is must to ensure IS. . To ensure appropriate levels of access, a variety of security measures must be instituted based on business needs and as recommended by the Chief IS Officer.

Policy Statement

Mechanisms to control access to confidential information and IT assets shall include all sites situated within the bank. The assets shall be protected against unauthorized environment and physical threats. For this purpose the bank will give clear guidelines on authority and responsibility for its employees and other authorized stake holders to access the information and IT assets. Bank employees will strictly adhere to these norms/guidelines. Detailed rules on this regard will be issued by the bank.

3. Acceptable Usage Security

Purpose

The purpose of this policy is to clarify users' rights, responsibilities, information assets and rights, to shield the organization against potential threats and liabilities. Bank assets are provided for business purpose. User of information is expected to access information only in support of authorized job responsibilities or role.

This will

- Minimize security threats by promoting awareness and good practices
- Encourage effective and positive use of information assets and resources.
- Ensure that users follow safe usage practices that do not hamper business objectives, not to bring disrepute or to attract legal liability

Policy Statement

Bank assets are l be provided for business purpose and not for the personal use of its employees or other authorized users of information and information assets. To ensure this users shall follow to safe usage practices that do not hamper business objectives, bring disrepute to or attract legal liability. Violations to the usage policy by an employer /user will attract strict action and penalties including disciplinary action.

4. Incident Management

Purpose

IS incident could be a single or a series of unwanted or unexpected IS events that have a significant probability of compromising business operations and threatening IS. IS incidents are those which impact I T security. Incident management call for plan and procedures to deal with the incidents so as to protect the information and or information assets. The purpose of this policy is to develop and implement processes for identifying and responding to IS incidents. The CISO and his/her team shall conduct reviews to identify reasons for IS incidents, evaluate the same and also develop corrective and preventive actions to manage and /or avoid recurrence of the incidents. .

It is necessary that IS events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Policy Statement

Every employee and user must report such IS events (breach or attack) to his/her immediate supervisor and also to the IS department. The banks IS committee, based on the CISO recommendations define roles and responsibilities for the department heads, branch heads to identify, and manage IS incidents. Events, incidents and problems should be reported to the appropriate authority. Persons vested with the responsibility should respond promptly with a view to contain loss and damage if any and to avoid reoccurrence.

5. Asset Classification & Handling

Purpose

Bank provides the medium for the purpose of exchanging transaction details through clients/ servers. Failure to properly protect information could have serious effect on the bank. As such, they would have to be protected with stringent security controls.

Information is classified to ensure its proper protection. Immediately after information has been created, modified or acquired, information must be evaluated to determine its classification. Also it should be decided as to how it must be handled. Information asset is any asset that has value for bank & consequently needs to be suitably protected.

Policy Statement

Every employee and authorized functionaries of the bank has responsibility in protecting the information asset from unauthorized access, generation, modification, disclosure, transmission or destruction. This is achieved by strictly following laid down procedures. In

Order to ensure that the security, reliability, integrity & availability of information is not compromised bank has laid down specific procedures and rules for each information activity. Bank will specify authority for appropriate asset handling. Schemes for labels shall be adapted by the bank for marking guidelines for IS.

6. Asset-Media Disposal

Purpose

Information can be compromised through careless disposal or re-use of media. Storages devices containing sensitive information should be physically destroyed or security overwritten. Rather than using the standard delete functions, all storages media should be checked prior to its disposal to ensure that sensitive data and licensed software, if any is not remained. It should be ensured that such data or software is either removed or overwritten.

Policy Statement

Employees, users and authorized officials of the bank shall ensure that banks owned computers, devices storages media shall have all data and licensed software reliable erased from all device at the time of disposal of the media or its movement out of bank control using best practices for each type of media.

7. Anti- Virus

Purpose

Bank must be protected against vulnerability due to virus and attack by Trojans and malicious codes. Hence IT assets of the bank must use enterprise level anti-virus solutions on the system. Appropriate Antivirus solutions approved by the Chief IS Officer and must be deployed for protecting against virus attack and Virus checking. Wherever possible a multi-layered approach should be used (desktops, servers, gateways, etc.) that ensures that all electronic files are appropriately scanned for viruses. Users (employees and other stake holders) are not authorized to turn off or disable virus checking.

Policy Statement

Malicious codes are viruses, worms , Trojans, root kits etc. represent significant threat to performance secrecy. Bank shall ensure that these malicious codes are detected early and removed. . These guidelines shall protect IT assets of the bank against malicious code through enterprise level anti-virus solution. Bank will use an appropriate antivirus solution and keep it updated on a regular basis.

8. Networking & Internet Security

Purpose

Protecting Networking infrastructure against threats and mitigating such threats originating from external, and internal network is of prime importance of the bank. Absence of proper access control and protection can lead to internet based attack that includes unauthorized access from internet; spread of virus, worms, malware, etc. There could be unsecured

transit on the network that can lead to unauthorized access leading to loss of critical & sensitive information.

It is necessary to provide secured access to the bank's network to internal and external users, provide adequate redundancy for critical IT assets & establish effective management of the networking infrastructure.

Policy Statement

Enterprise network infrastructure shall be appropriately designed, and managed and controlled effectively in order to ensure protection of the information in the network as also of the for support infrastructure. All connections to extended network including Internet, outsourced Vendors and partners shall be authorized and provided in a secure manner. All remote access to the network shall be authenticated & provided based purely on business requirement. Network should be designed & maintained for high availability and to meet the requirement of the User.

9. Operating Systems

Purpose

To determine appropriate risk response options, identify performance gaps between current and desired risk level. Risk associated with IT systems whether appropriate and effectively mitigated to an acceptable level by securing Operating Systems.

Policy Statement

Operating systems shall be installed and configured in a proper manner. Operating system shall only be accessed by authorized users (employees and others) and un-authorized will be denied by using appropriate technology and other process ensuring confidentiality, integrity and availability.

10 Applications

Purpose

Applications are vulnerable to various kinds of attacks, which are exploited by a malicious activity. Computer software owned or licensed must not be copied by users; employees and others for use at home or any other location. Exceptions to this will be specifically authorized by the Information Owner. Anyone could access information and/or data wherein security controls like authentication mechanism can be easily bypassed. Hence, it is imperative that Security controls to protect the application are appropriate and deployed on a continuous basis.

Policy Statement

Application deployed in bank shall have controls for secure input processing, through system, storage and output of data. Application shall be tested for security performance before deployment & for high availability. Access to application shall be restricted to authorized persons & access will be o provided on the principle of least privilege.

11. Database

Purpose

Bank's database contains critical and confidential business information of its constituents which have to be protected at all times. Hence, it has to be ensured that database is configured to protect client information and at the same make them available to authorized users on authentication. The organization needs to define and develop adequate controls to secure its database.

Policy Statement

The technical team (I T department) shall implement database system configured as per best security practices. Adequate controls to maintain confidentiality, integrity and availability of database at all times shall be put in place. User access to database shall be provided as per authorization and based on authentication. Database access will be given strictly based on business, operational needs and requirement.

12. Patch Management

Purpose

The hardware having computers and applications should be frequently patched to protect against widespread worms, malicious code that target known vulnerabilities on non-patched systems, resulting in downtime & business impact on banks.

The down time and business impact can be avoided by have effective patch management which will keep updated the IT system and applications deployed in the bank.

Policy Statement

The bank shall be secured against known vulnerabilities in operating systems and applications software through an effective patch management process.

13. Back-up

Purpose

Back-ups of essential information, data and software shall be taken on regular basis, one copy on site and one off-site. This should to be strictly followed to ensure that all essential information and SW could be recovered in the event of a disaster or failure of media. This would help to prevent loss of data which can impact in terms of delay, increased costs, loss of credibility & embarrassment.

Policy Statement

Information system/asset owners (employees) shall ensure that adequate back-ups, as per stipulated periodicity are taken so that the data is not lost and can be recovered, in the event of an equipment failure, intentional destruction of data, or disaster. The IT department shall be responsible for operationalsing this policy.

14. Personnel

Purpose

People are the key assets in creating, storing, maintaining, distributing, processing and protecting the information/data of the organization. All employees as also contractual users should adhere to all the IS security guidelines and access information purely based on job responsibilities and requirements. They should not access information for personal use. The access can be revoked or modified with changes in such responsibilities.

Policy Statement

People are the key assets in creating, storing, and maintaining, distributing, processing protecting. All employees as also contractual users shall adhere to the Personnel Security and access based on responsibilities. The access can be revoked or modified with changes in such responsibilities

Bank shall ensure that each employee is made aware of the importance of IS and their role in ensuring IS. Also employees will be instructed to strictly adhere to various IS related instructions and not to use information for other than official purposes. Employees will be informed of their access and other rights which can be revoked in the event of role changes.

15. Password

Purpose

If an authorized user or a customer who is not authorized gains access to banks information and information assets, it could result into loss of confidence constituents and result in compromise with integrity of data.

Generally the user and customer gain access to information/data through user-ID and the password provided for securing transactions. Access to systems should be strictly limited for the genuine business purposes with the complement of User ID and password

Policy Statement

Every user shall be assigned a unique User ID. Users both employees and customers shall choose/create their passwords in accordance with policy and shall protect at all times during its generation, delivery, storage and usage. The password change process shall be well calibrated. Users and Customers will be mandated to periodically change the password. Bank will educate the customer on the need for confidentiality in the password, not sharing it with others and the consequences of sharing the password.

16. E-mail Usage and Security

Purpose

The e-mail system for the bank is required for day-to-day function for genuine banking and operations. It is also a part of the customer service. A lot of internal information is shared with employees and functions/function heads through email. As such appropriate controls have to be provided for security for e-mail.

Policy Statement

E-mail ID and access shall be made available to employees purely based on business needs. Every employee shall develop a password for accessing the mail. Email activity shall be protected adequately to provide availability, exchange of information between employees of the bank and with the third parties. Bank will protect the system with appropriate technology and other means against breach or unauthorized access. Employees will not be allowed to use email for personal work.

17. Change Management

Purpose

Unauthorized changes and ad-hoc changes in the IT and other electronic systems could lead to system getting interrupted and result in genuine persons and users unable to access system or information assets. It is laid down that major or minor changes to any information assets where ever necessary should be carried out with prior approvals. The changes are to be identified and monitored. The entire process will have to be documented. It is provided that changes will be implemented in test environment before taking to production.

Policy Statement

Changes to the IT systems shall be performed in controlled manner. To ensure that the risk associated with changes are managed to an acceptable level, changes will be made only after careful consideration of its need, impact and proposed changes will be thoroughly tested before these are deployed.

18. Monitoring

Purpose

IT infrastructure components form a crucial part of assets of the banks. IT assets are constantly under threat from hackers and other malicious users and as a result needs to be monitored effectively on a continuous basis for identifying any abnormal activities and for the purpose of protecting the asset. The effectiveness and applicability of IS controls have to be monitored based on control testing criteria, purpose of testing and results periodically reported to the management. Security controls need to be continuously implemented on IT assets to protect them from unforeseen threats.

Policy Statement

The bank shall establish an effective enterprise level system to centrally monitor IS controls. All access to critical applications and banks network shall be monitored for suspicious activities or security breaches. Adequate response mechanism shall be set up for controlling security breach, if any.

19. Outsourcing/Third Party

Purpose

There are a number of IT based activities that the bank has outsourced. These include AMC for hardware and software, maintaining ATM etc. The bank is aware of the risk of improper access to information and information assets from users of third party or outsourcing agencies which could prove detrimental to banks interests. A risk assessment exercise should be carried out to determine the specific security requirements in such cases. Contract with third parties or outsourcing agencies should be established with necessary security conditions and service levels in mind.

Policy Statement

Banks shall ensure that access to the data processing facilities and Intellectual property rights of the bank are well protected from third party service provider's entities and controls by taking adequate measures.

20. Business Continuity

Purpose

To fulfill the bank's commitment to protect its customers and in the interest of rendering uninterrupted banking services it would be prudent for the bank to thwart all kinds of threats to its business which could have the potential to disrupt its operations. In other words bank should ensure robust systems such that its business continuity is not threatened. In view of this, critical information systems of the bank should be planned and suitably designed to ensure continuity of operations, even in the event of a disaster. IS is one such critical aspect. Thus the purpose is to counter interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Policy Statement

Bank shall ensure the safeguard of its information and information assets to minimize the risk, costs & duration of disruption to business operations. Bank will establish and maintain integration between response plans, DRP & BCP. Bank will have a plan for effective continuity of business & a well-rehearsed recovery process or a combination of these which will enable the resumption of critical business activities.

21. ATM

Purpose

The objective of this policy is to prevent misuse and minimize security risks to ATMs installed in the bank premises and at off-site locations. The ATMs being an important delivery channel offering financial and non-financial services, the security risks must be considered on top priority for prevention of frauds.

Policy Statement

A network of ATMs exists in the bank where a secret ATM operation code will be issued to the customer in the form of Personal Identification Number i.e. PIN for ATM operations. The concept of PIN prevents an unauthorized user from gaining access to the ATM network as a combination of physical card and PIN number is required for accessing the account

for withdrawal of cash and/ or any other services offered by bank through card and ATM. ATMs will also be guarded suitably against theft, unauthorized access etc.

PART II

INFORMATION SYSTEMS SECURITY POLICY

POLICIES AND PROCEDURES

For all the policies stated in part I the descriptions and procedures are given below.

2. Environment and Physical Security Policy

Purpose

Control of Physical and electronic access to confidential information and computing resources is must to ensure IS. To ensure appropriate levels of access, a variety of security measures must be instituted based on business needs and as recommended by the Chief Information Security Officer (CISO).

Policy Statement

Mechanisms to control access to confidential information and IT assets shall include all sites situated within the bank. The assets shall be protected against unauthorized environment and physical threats. For this purpose the bank will give clear guidelines on authority and responsibility for its employees and other authorized stake holders to access the information and IT assets. Bank employees will strictly adhere to these norms/guidelines. Detailed rules on this regard will be issued by the bank.

Procedures: Scope

All sites, which house bank's critical IT assets, shall provide resistance to unauthorized physical access and have protection against environmental threats. All physical access and movement of IT assets shall be monitored and reviewed.

Access Control

2.4.1 All critical information processing facilities shall have adequate protection against unauthorized access.

2.4.2. Every employee shall be provided with name, identification/access cards consisting of banks name the details of time of arrival, duration of the activity, and reasons of access shall be recorded. In case of emergency, approval for access can be given on the phone or e-mail with a proviso that detailed request form shall be sent after activity.

Access to secured areas shall be allowed only after necessary approval.

A log book shall be maintained to track all access to critical information processing facilities.

An updated list of personnel who have access to critical information processing facilities shall be maintained.

Security guards must check IT equipment and media carried by all personnel entering or leaving information processing facilities.

Visitors, vendors and external people shall be accompanied by bank staff when working in critical information processing facilities.

An access control register shall be maintained at the entry point of Data Centre.

People who are not Data Centre employees and third party (external) visitors shall make appropriate entry in the register before entering.

2.5 Environmental Protection

There shall be adequate provisions for fire - detection, fire fighting and control.

All personnel shall be trained for fire-fighting.

Air Conditioning Systems shall be implemented to ensure that the operational environment conforms to the equipment manufacturer's specifications.

All critical equipment such as air conditioners, gen-sets, etc. shall remain under Annual maintenance contract, at all times.

Data Centre Security

4. Critical processing area in Data Centre shall be accessed only by authorized personnel. They alone will be allowed inside/access.

5. Emergency exit shall be provided in the data centre for use in emergency situation (it shall not be available as a matter of routine).

Identification of Devices

For easy identification, data cables and electrical cables must be properly labelled.

Proper labeling of racks shall also be ensured. All devices shall also be similarly numbered (as contained in the racks). Rack number shall form part of the device identification number which must be pasted on all devices.

CCTV Monitoring

CCTV monitoring systems shall be installed at the Data Centre and a proper monitoring system shall be put in place at entry and exit points at the Data Centre as also in area having critical IS assets. The CCTV footage shall be maintained – kept on record for a specific period – a Minimum period of 90 days.

Power at the Data Centre

Power Systems shall be designed and provided to ensure uninterrupted and quality power supply at the Data Centre. UPS shall be provided for backup.

UPS Systems shall be checked once in a quarter or as recommended by the manufacturer for its proper functioning/efficacy. Additionally, test checks shall also be carried out, on a quarterly basis.

2.9.3 A backup power system shall be provided to all access control systems, physical security systems such as fire and smoke alarms, emergency lighting systems, fire detection & suppression systems, etc.

2.9.4. The electrical power supply to the Data Centre shall be segregated from other power

circuits of the building. Similarly, the power supply to the IT equipment/assets at the Data Centre shall be segregated from all other equipment.

2.9.5 Switches shall be provided in easily accessible locations within the Data Centre and outside the Data Centre to be used to switch off the power, in case of an emergency.

Fire Prevention and Control

Infrastructure at the Data Centre shall be erected from fire-resistant material. Automatic fire detection systems shall be installed for detection as also for alerting. Gas based fire suppression systems shall be installed to control outbreak of fire. Fire detection and suppression systems shall be capable to automatically shut off electrical power.

No combustible material shall be provided or stored at the Data Centre.

Basic training on fire-fighting techniques shall be provided to staff at the Data Centre. Periodical fire-drills shall be conducted, as per the security policy of the bank.

Environmental Safeguards

Temperature and humidity shall be monitored and controlled at the Data Centre.

Air shall be filtered and circulated to remove dust and contamination at the

Data Centre.

Water/Moisture detectors shall be placed below the false floor in the Data Centre, if the area is prone to moisture and water seepage.

Raised false floor shall be erected to provide proper environment, temperature,

cabling, etc. 2.11.5. The Data Centre shall always be maintained dust and dirt-free.

Preventive Maintenance

a. Preventive maintenance of all equipment, electrical installations, alarm systems, back-up power supply, UPS, etc. shall be carried out periodically.

b. Proper monitoring of such maintenance by personnel posted at the Data Centre shall be ensured.

Monitoring

a. Automatic alerting systems shall be installed at all access points to critical information processing facilities.

b. Monitoring systems shall be deployed to track any suspicious activity.

Document Security

a. Sensitive documents shall be stored in locked cabinets.

b. Fax machines and printers shall be protected against unauthorized access.

Enforcement

Compliance with the security policies of the bank shall be a matter of periodic review by the ISC. Any employee found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment as deemed appropriate by the management of the bank.

3. Acceptable Usage Security

Purpose

The purpose of this policy is to clarify users' rights, responsibilities, information assets and rights, to shield the organization against potential threats and liabilities. Bank assets are provided for business purpose. User of information is expected to access information only in support of authorized job responsibilities or role. This will

- Minimize security threats by promoting awareness and good practices
- Encourage effective and positive use of information assets and resources.
- Ensure that users follow safe usage practices that do not hamper business objectives, not to bring disrepute or to attract legal liability

Policy Statements

Bank assets are l be provided for business purpose and not for the personal use of its employees or other authorized users of information and information assets. To ensure this users shall follow to safe usage practices that do not hamper business objectives, bring disrepute to or attract legal liability. Violations to the usage policy by an employer /user will attract strict action and penalties including disciplinary action.

Procedures for Acceptable Users and Usage Security: Scope

Users' rights, responsibilities, information assets and rights shall be specified to shield the organization against potential threats and liabilities. Minimize security threats by promoting awareness and good practices. Encourage effective and positive use of information assets and resources.

Desktop Users

- All desktops shall be configured by system administrators as per the secure configuration standards provided by IS Committee (ISC).
- Users shall not install any software or applications on their desktop that is not authorized or not essential to bank's business.
- Users shall not connect modems to their machines unless and otherwise approved by the appropriate authority.
- Necessary measures shall be adopted by users to prevent the risk of unauthorized

access.

- Desktops as also external devices like CD, pen drives, etc. shall be configured by IT teams in accordance secured configuration by IT team be as per standards.
- Users shall not install any software, application on their desktop that is not authorized. Users can effect changes in the desk top only through IT department.
- Approved products only can be installed on desktops/laptops.
- The servers shall be configured and maintained only by the I T department or authorized officials.
- Internal LAN shall be segregated from the external Internet. User shall not connect through modems. Also for connecting to external access, network team will configure all desktops as per secure configuration.
- User must log out of all applications when leaves; if not used, desktop shall automatically log-out for extended period of time.
- Screen saver shall be enabled with Password. Access through pass word is essential if the PC is unattended for short time.
- It should be ensured that there is sharing in any user's folders in desktops over network.

Laptop Users

- Laptop users need to adopt the following measures
- Ensure that laptop is configured as per the secure configuration documents provided by ISC.
- Enable boot level password in the laptop.
- Encryption or password protection shall be enabled for protection of data.
- Antivirus agent with latest signatures shall be installed, before laptop is connected to the LAN.
- All necessary patches / hot fixes for the operating system and applications installed shall be periodically updated.
- Log off laptops when not working for extended period and enable screen saver with password for protection during short period of inactivity.
- Backup critical files from laptop to Users' desktop or removable media like CD/Pen drives
- User to take adequate measures for physical protection of laptop including not leaving laptops unattended in public places or while traveling.
- If the laptop has modem / dial up facility for Internet, users shall disconnect Internet connection before connecting to the bank's LAN.
- Loss of laptop shall be reported immediately to the department head and ISC.

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

- Laptops Security– Configuration as per policies shall be carried out by security team.

- Enable booting passwords and additional protection.

- Shall take precaution for physical protection by backing up critical files to central server.

- The system shutdown option which allows users to shut down the system without logging in first, will be restricted on all servers housing sensitive information.

- A logon banner shall appear on all information systems prior to login on to the system stating that the information system shall only be accessed by authorized users and un-authorized access is prohibited, monitored and liable for punitive actions.

- The number of unsuccessful logon attempts will be limited to (say five) after which the system will lock that particular User ID. All unsuccessful login attempts will be recorded.

- On completion of a successful log-on the following information will be logged: (a) date and time of the previous successful log-on (b) details of any unsuccessful log-on attempts since the last successful log-on.

Password Security

- Users (employees and other authorized personnel) are responsible for all activities originating from their computer accounts.

- Users shall choose passwords that are easy to remember but difficult to guess.

- Protection

- Users shall not disclose/share their passwords with anyone including colleagues and IT staff

- Users shall ensure that nobody is watching when they are entering password into the system

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

- Users shall change their password regularly.

- User shall report to the system administrator if account is locked out before 3 bad

attempts.

Internet Usage

- Internet access is provided to users for the performance and fulfillment of job responsibilities.
- Employees shall access Internet only through the connectivity provided by the bank and shall not set up Internet access without authorization from IT department.
- All access to Internet will be authenticated and will be restricted to business related sites.
- Users are responsible for protecting their Internet account and password.
- In case misuse of Internet access is detected, bank can terminate the user Internet account and take other disciplinary action as bank may deem fit.
- Users shall ensure that security is enabled on the Internet browser.
- Users shall ensure that they do not access websites by clicking on links provide in emails or in other websites.
- Bank reserves the right to monitor and review Internet usage of users to ensure compliance to this policy.

Clear Desk

- While users work in an online environment, at times they are required to use papers/ storage devices for information exchange. Information on important customers & sensitive business data is also available on other media like computer generated printouts, office papers, CDs, pen drives, diskettes etc.
- Cabins/ Desks & meeting rooms with papers piled high not only poses fire risk but also may be in legal breach for not preserving confidentiality of customer information. The act places a legal obligation on employees concerned to protect sensitive personal information.
- To prevent such data leakage due to non-clean desks, user/ authorized personnel shall ensure that confidential documents and media files are not left unattended. Unused documents/ papers shall be destroyed using shredder machine.

4. Incident Management

Purpose

IS incident could be a single or a series of unwanted or unexpected IS events that have a significant probability of compromising business operations and threatening IS. IS incidents are those which impact IT security. Incident management call for plan and procedures to

deal with the incidents so as to protect the information and or information assets. The purpose of this policy is to develop and implement processes for identifying and responding to IS incidents. The CISO and his/her team shall conduct reviews to identify reasons for IS incidents, evaluate the same and also develop corrective and preventive actions to manage and /or avoid recurrence of the incidents. It is necessary that IS events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Policy Statement

Every employee and user must report such I S events (breach or attack) to his/her immediate supervisor and also to the IS department. The banks IS committee, based on the CISO recommendations define Roles and responsibilities for the department heads, branch heads to identify, and manage IS incidents. Events, incidents and problems should be reported to the

Appropriate authority. Persons vested with the responsibility should respond promptly with a view to contain loss and damage if any and to avoid reoccurrence.

Scope

Maintain processes to investigate and document incidents to be able to respond appropriately. To determine their causes, adhere to legal regulatory and organizational requirement.

Incident Identification

All users and administrators of IT systems shall be responsible for identifying incidents. An incident is the act of violating an explicit or implied security policy. The following actions can be classified as incidents:

i. Attempts to gain unauthorized access to a system or its data; masquerading, spoofing as authorized users.

ii. Unwanted disruption or denial of service.

iii. The unauthorized use of a system for the processing or storage of data by authorized users.

iv. Changes to system hardware, firmware or software characteristics and data without the owner's knowledge, instruction or consent.

v. Existence of stray user accounts.

Incident Reporting

If a user suspects that an incident has occurred, it shall be reported immediately to the branch system administrator / department head or to the helpdesk. The administrator shall do a preliminary analysis to ascertain the cause and extent of damage.

An incident report shall be sent to the IS Committee (ISC) containing the following details

- Description of the incident
- Possible causes
- Damages observed
- Supporting evidence
- Remedial steps taken

Based on data available and level of criticality of incident, ISC shall send out incident alerts to application groups and user departments which could possibly be affected by similar incidents.

4.5.4 Users of the IT system shall report security incidents identified.

4.5.5. Users are required to provide their identity and contact details while reporting incidents for effective follow up.

Incident Verification

The ISC shall analyse the incidents based on the data received from the administrator. The ISC shall seek more information from the system administrators, if required.

The ISC shall record the incident and allocate an incident number for tracking and future reference.

Once the incident validity has been verified, ISC shall draw up an action plan.

Head of IT shall be updated about the incident, impact on business and proposed action plan

Incident Recovery

System personnel required for executing the recovery plan shall be contacted by the application team.

Additional monitoring mechanisms shall be deployed for a short duration of time after recovery to ensure that all incident related activities have ceased.

Incident Prevention

Based on the learning from the incident, ISC shall make necessary changes (if required) to security policies.

ISC shall maintain a database of incidents and recovery steps.

5. Asset Classification & Handling

Purpose

Bank provides the medium for the purpose of exchanging transaction details through clients/servers. Failure to properly protect information could have serious effect on the bank. As such, they would have to be protected with stringent security controls.

ISO 27001 is an international standard that helps financial institutions manage information security. It provides a framework for identifying and managing risks to data, systems, and assets.

How does ISO 27001 help financial institutions?

- **Risk management**: Helps banks identify and assess risks like cyber-attacks, data theft, and system failures
- **Asset management**: Helps manage the security of assets like financial information, intellectual property, and employee details

- **Security controls**: Helps implement best practices to protect sensitive data
- **Compliance**: Helps comply with international security standards and legal obligations
- **Continuous improvement**: Helps ensure that security measures are robust and continually improved

How is ISO 27001 implemented?

- ISO 27001 is structured around an information security management system (ISMS)
- The ISMS integrates organizational, technical, and physical controls
- The ISMS is based on a comprehensive approach that considers people, policies, and technology

The NIST Cybersecurity Framework (CSF) is a set of guidelines that helps banks and other organizations manage and reduce cybersecurity risks. The framework is flexible and can be tailored to meet the specific needs of an organization.

How the NIST CSF can help banks

- **Identify risks**: Banks can use the CSF to identify risks based on their systems, products, and stakeholders
- **Assess cyber security**: The CSF helps banks assess their current cybersecurity practices and sophistication
- **Prioritize risks**: Banks can use the CSF to prioritize risks and determine where to focus their cyber security efforts
- **Develop policies**: Banks can use the CSF to develop cyber security policies and practices
- **Train employees**: Banks can use the CSF to train employees on cyber security best practices
- **Monitor risks**: Banks can use the CSF to monitor cyber risks and implement controls to mitigate them .

CSA FRAMEWORK & ISO 27701

Scoping is so delicate with all compliance initiatives, it's no wonder that organizations run into problems scoping their ISO 27701 privacy information management system (PIMS) too.

The PIMS is an extension of your ISO 27001 information security management system (ISMS), so **when you go about defining its scope/boundaries in the context of the processing of personal data, remember this:**

- The PIMS scope can be narrower than that of the ISMS, but it cannot be broader.
- It also may be narrower than your privacy program as a whole.
  - If a particular system, process, or application is not in the scope of the ISMS, then it cannot be included in the PIMS scope (though it may be part of your overall privacy program.)
    - For example, your marketing activities may fall within the scope of your privacy program but may fall outside the bounds of your ISMS. So those activities could not be included in the PIMS (unless you extended your ISMS to include marketing).

As you create and define these boundaries, you'll face a key decision point: Do you fold the PIMS requirements into existing ISMS documentation or create standalone documentation?

- The case for folding in:
  - If your ISMS / PIMS is one combined management system, you should be able to easily incorporate the PIMS scope into the ISMS documentation.
  - You avoid the efforts of duplicative documentation and can also consolidate updating both sets for relevant changes.

  The case for additional documents:
  - You'd be less likely to miss/exclude areas regarding PIMS/ISO 27701/privacy references.

Information is classified to ensure its proper protection. Immediately after information has been created, modified or acquired, information must be evaluated to determine its classification. Also it should be decided as to how it must be handled. Information asset is

any asset that has value for bank & consequently needs to be suitably protected.

Policy Statement

Every employee and authorized functionaries of the bank has responsibility in protecting the information asset from unauthorized access, generation, modification, disclosure, transmission or destruction. This is achieved by strictly following laid down procedures. In order to ensure that the security, reliability, integrity & availability of information is not compromised bank has laid down specific procedures and rules for each information activity. Bank will specify authority for appropriate asset handling schemes for labels shall be adapted by the bank for marking guidelines for IS.

Scope

Information assets apply to all users of the bank housed with the institution as and/or with the outsourced/ third parties.

Accountability

5.4.1 All major information assets like application software and databases shall have a nominated Data Owner.

5.4.2. The Branch Head/ Regional Head/ Administrative Office Head will initiate measures for nominating functional owners for all major information assets of bank.

Information Classification

All information system assets will be classified under one of the following categories:

Secret Information: Secret Information is highly sensitive to internal and external exposure.

Confidential Information: Confidential Information is sensitive to external exposure, the unauthorized disclosure of which would cause administrative embarrassment or difficulty.

Corporate Confidential Information: Any confidential information of the Bank's internal affairs, which cannot be shared with employees, Branches / Regional / Administrative Offices, unless, needed for the purpose of routine operations or conducting business.

Branch/ Regional/ Administrative Office Confidential Information: Any confidential information, which can be shared across Branches/ Zones/ Administrative Offices, but is not intended to be shared as Public Information, will be classified as Branch/ Regional/ Administrative Office Confidential Information. Public: Public Information includes information such as various services, marketing brochures and promotional literature, advertising media and Bank web sites.

A given security classification cannot be downgraded to a lower category except by the Data Owner.

Document Classification

Appropriate security classification will be clearly stated for all hardcopy collections of

documents consistent with the information classification, except for Public information. The following classification standards will be maintained.

Secret Documents: Secret documents will be marked as ‘SECRET’ on the first/heading page.

Confidential Documents: Confidential documents will be marked as ‘CONFIDENTIAL’ on the first/heading page.

General Documents: All un-labelled documents will fall into this category.

Media Handling

All computer media like tapes, disks, CDs pen drive etc. will be stored in a safe, secure environment, in accordance with the manufacturer's specifications.

Procurement, distribution and use of blank CDs, tapes, pen drive/floppies, etc. will be inventoried and controlled by the respective Administrative Head.

No printed output or removable media will be taken out of the office premise unless authorized in writing by the respective Administrative Head with a copy to the Gate Security In-charge, if any, wherever practical.

No printed output or removable media containing, Secret or Confidential data will be taken out from the Computer Room premises unless approved in writing by immediate controlling authority.

Personal media like tapes, disks and cassettes will not be carried and used in the office premise.

Inventory of software media containing system software, operating system and such other software and application utilities will be maintained.

Enforcement

Compliance with security policies will be a matter for periodic review by the ISC. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as deemed appropriate by the management.

6. Asset-Media Disposal

Purpose

Information can be compromised through careless disposal or re-use of media. Storages devices containing sensitive information should be physically destroyed or security overwritten. Rather than using the standard delete functions, all storages media should be checked prior to its disposal to ensure that sensitive data and licensed software, if any is not remained. It should be ensured that such data or software is either removed or overwritten.

Policy Statement

Employees, users and authorized officials of the bank shall ensure that banks owned computers, devices storages media shall have all data and licensed software reliable

erased from all device at the time of disposal of the media or its movement out of bank control using best practices for each type of media.

Scope

This policy is applicable to any electronic information storage or paper- based media containing internal use classification or confidential data.

Policy applies to all employees and third party personnel who have access to, develop, use, copy, print, exchange information, earlier internally within the organisation or externally with third parties.

Policy applies also on all I T Assets

Policy also applies on the employees of the third party who are involved in the disposal procedure.

6.4. Disposal of Information Assets

Media containing sensitive information (Secret or Confidential) will be disposed of securely and safely when it is no longer required e.g. by incineration or destroyed by securely deleting. Such disposals will be authorized by the Administrative Head at the location.

Disposal of Electronic Media

The departmental heads are responsible for overseeing compliance with data and disk disposal in his or her area on a yearly basis.

Information on storage media like hard disk drives or removable media like tape drives, USB, CD drives shall be formatted or erased three times if the media is to be reused.

Low level formatting shall be done for hard disk drives of all desktops and laptops three times before reusing or sending them for maintenance.

Magnetic media like floppy disk, hard drives, zip disks, etc. shall be erased using a degaussing device or disk wiping software before being discarded.

Expired or corrupted storage media like floppy, CDs or tape/optical media shall be degaussed or erased prior to its disposal.

Optical tape drives, internal hard drives and RAID arrays shall be wiped out using department or organisation's 'disk-wiping' software, since a simple delete, erase, re-format or disk command for Windows is not sufficient as there are many products which can retrieve erased data and software. Additionally, such drives shall be physically destroyed either within the organisation or via an external media disposal third party service.

Disposal of Paper based Media

Department/Branch heads shall nominate an official from the department/branch who would be responsible for overseeing paper-based document disposal in his/her area.

All waste copies of sensitive information that are generated in the course of copying, printing, or faxing need to be shredded using paper shredders/incinerators or shall be placed in locked bins clearly marked as containing confidential data.

Confidential and restricted data and paper documents shall be destroyed using paper shredders or incinerators.

Condition for disposal of IT Assets

The condition of the asset and not its age shall determine its usefulness or obsolescence. The circumstances under which IT assets may be considered for disposal are –

When no economic benefit can be derived from active use of the asset. When maintenance cost of an asset exceeds its replacement cost.

Up gradation of an asset is no longer possible.

Replacement or disposal reduces cost of operations and improves efficiency. Due to change in technology and market conditions, it is no longer functional.

Certification of usefulness or utility shall be obtained from technical expert.

Disposal of IT Asset - Procedure

Following procedure shall be followed for disposal of IT asset:

All proposals requesting for disposal of IT assets at departments/branches shall be submitted by the Head of the Department/branch to the IT head.

7.8.2. While disposing of IT assets, departments will ensure that necessary backup of data has been taken for future use. It should be ensured that information if any in the asset is deleted before the asset is disposed off.

Periodicity of disposal of obsolete IT Assets

Disposal process shall be carried out on a yearly basis. However, if immediate need of disposal is felt, assets can be disposed off as and when required with the approval of the IT head.

Outsourcing of Disposal of IT Assets

If disposal of IT assets is outsourced, external contractors responsible for general disposal arrangements, bank shall have or insist on proper security and process checks to ensure that information assets are disposed off in a secure manner. Disposal of confidential and internal items shall be logged, in order to maintain an audit trail. Disposal of confidential/restricted labelled information assets or documents shall be done securely and shall be witnessed by the custodian.

Non-disclosure agreement shall be signed between the bank and the external contractor while outsourcing disposal of IT assets.

Certificate of secure disposal shall be obtained from external contractor.

6.11. Enforcement

Compliance with the Security Policies will be a matter for periodic review by the ISC. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as deemed appropriate by the management of the bank.

7. Anti-Virus

Purpose

Bank must be protected against vulnerability due to virus and attack by Trojans and malicious codes. Hence IT assets of the bank must use enterprise level anti-virus solutions on the system.

Appropriate Antivirus solutions approved by the Chief IS Officer and must be deployed for protecting against virus attach and Virus checking. Wherever possible a multi-layered approach should be used (desktops, servers, gateways, etc.) that ensures that all electronic files are appropriately scanned for viruses. Users (employees and other stake holders) are not authorized to turn off or disable virus checking.

Policy Statement

Malicious codes are viruses, worms, Trojans, rootkits etc. represent significant threat to performance secrecy. Bank shall ensure that these malicious codes are detected early and removed. These guidelines shall protect IT assets of the bank against malicious code through enterprise level anti-virus solution. Bank will use an appropriate antivirus solution and keep it updated on a regular basis.

Scope

All desktops and server machines in the bank shall have anti-virus installed. This does not include server machines with UNIX server like operating systems where the risk of virus infection is very less.

Installation

Anti-virus agent installation shall be password protected.

Anti-virus agent shall be configured to do a full system scan at least once a day.

Anti-virus agent shall be configured to do a real time scan of all the files when these are accessed, copied or moved.

Anti-virus agent shall be configured to quarantine the infected files if they cannot be

cleaned.

Anti-virus on the email servers shall be configured for scanning all internal and external mails

Anti-virus on the Internet gateways shall be configured to scan all the incoming/outgoing Internet traffic.

Anti-Virus Support Team

There shall be a dedicated Central Anti-virus Team (CAT) for managing the entire anti-virus infrastructure for systems connected to core banking network.

There shall be a dedicated central anti-virus administrator for managing the anti-virus infrastructure for systems in non-core banking network (TBM, non-core, non-core-ATM).

Anti-Virus Signature Update

New signatures shall be applied as soon as they are released by vendor. Anti-virus application architecture of the bank shall ensure that new signature updates reaches all machines connected on bank's core banking network within a day. In case of branches where signature updates are sent by CD it may take more than one day.

All systems connected on bank's core banking network shall be configured for automatic update from nearest anti-virus server.

All systems that are not on the core banking network shall be updated by the system administrator of the respective branch/ administrative office/ department.

Status Reports

Central anti-virus team (CAT) shall submit periodic reports on the status of anti-virus protection to the Product Manager - ISC.

Server Security

Operating System and applications on anti-virus servers shall be secured as per the secure configuration document.

Logical access to the anti-virus servers shall be restricted to the authorized personnel only.

Anti-virus servers shall be placed in a controlled physical access environment with access only to authorized personnel.

Server monitoring

System performance of anti-virus servers shall be monitored periodically.

The operating systems and application log files shall be monitored periodically.

Tracking new vulnerabilities

CAT shall be responsible for keeping track of any new vulnerability that could lead to worm or virus attacks on the network.

CAT shall take steps to mitigate the risks associated with new vulnerabilities.

Documentation

CAT shall maintain updated documents required for installation, configuration and administration of all anti-virus components.

CAT is responsible for distributing these documents to system administrators.

7.12. External Users

External users shall be allowed to connect laptops/desktops/palmtops to the bank's network only after ensuring that signature and patches are updated.

Backup and Redundancy

Backup of anti-virus application, configuration and log files shall be taken on a periodic basis

Test recovery shall be done periodically.

7.13.4. There shall be redundancy for critical anti-virus servers.

Reporting

Users shall report to system administrator if a virus is not getting cleaned by the anti-virus agent

In case of virus outbreak in the branch, the system administrator in the branch shall immediately notify the CAT.

8. Networking & Internet Security

Purpose

Protecting networking infrastructure against threats and mitigating such threats originating from external, and internal network is of prime importance of the bank. Absence of proper access control and protection can lead to internet based attack that includes unauthorized access from internet spread of virus, worms, malware, etc. There could be unsecured transit on the network that can lead to unauthorized access leading to loss of critical & sensitive information.

It is necessary to provide secured access to the bank's network to internal and external users, provide adequate redundancy for critical IT assets & establish effective management of the networking infrastructure.

Policy Statement

Enterprise network infrastructure shall be appropriately designed, and managed and controlled effectively in order to ensure protection of the information in the network as also of the for support infrastructure. All connections to extended network including Internet, outsourced vendors and partners shall be authorized and provided in a secure manner. All remote access to the network shall be authenticated & provided based purely on business requirement. Network should be designed & maintained for high availability and to meet the requirement of the user.

Scope

This policy applies to all assets comprising network devices, communication links, using network, servers and desktops and LAN and WAN infrastructure to be deployed and maintained by the bank. Internet and Intranet network are deemed forming part of bank's network infrastructure.

Internet Access

Internet access to users in the branches shall be provided from a central gateway located at Head Office (HO) or through dial up wherever centralized facility is not available.

Internet access shall be provided to users only after approval from business unit head or branch manager.

Internet access shall be controlled using IP address and user-id based authentication.

Internet connection shall be secured through a firewall.

Gateway level anti-virus shall be deployed to scan all the internet traffic.

Internet access shall be controlled to ensure that only sites required for business purposes are allowed.

All Internet access by the users shall be logged on the proxy whenever it is through Central Gateway.

Dial out Access

Users located in branches which cannot access internet through the central gateway can access Internet through Modem. The desktop/ systems used for dial-out connectivity shall be isolated from the rest of the user LAN and the bank's network.

Users shall take approval from the IT networking team and Information Systems Security Team (ISC) before using Modem.

WAN Access on Bank's Network

Access control list shall be implemented at the branches to prevent inter-branch access. Branches which require inter branch access must take approval from the ISO.

All confidential information shall be sent over the bank's network in encrypted format.

Segregating Server and User Segments

Business critical application servers shall be separated from the user segments by a firewall.

IDS shall be deployed to monitor all traffic to and from business critical servers and the delivery channels.

External Access

All branches, administrative offices and head office departments shall get prior approval from ISO before connecting with external networks that are outside the security management of the bank.

External networks shall be separated from bank's network through access control devices.

IDS shall be deployed to monitor the external traffic.

Dial in Access

All branches, administrative offices and head office departments shall get prior approval from ISO before providing dial-in access to the network.

Dial in access for product technical support shall take approval from ISC.

Any dial-in server shall be separated from the bank's network by means of an access control device.

Redundancy

Adequate redundancy shall be built in to the network links.

Redundant links shall have the same level of security as the primary

links 8.11. Network Device Configuration

Network devices such as Routers, Switches and Firewall shall be secured based on the secure configuration document (SCD) obtained from ISC.

8.12. Documentation

There shall be detailed documentation of the network architecture and the IP addressing

9. Operating Systems

Purpose

To determine appropriate risk response options and performance gaps between current

and desired risk level. Risk associated with IT systems whether appropriate and effectively mitigated to an acceptable level by securing Operating Systems.

Policy Statement

Operating systems shall be installed and configured in a proper manner. Operating system shall only be accessed by authorized users (employees and others) and un-authorized will be denied by using appropriate technology and other process ensuring confidentiality, integrity and availability.

Scope

All branches and administrative offices of bank shall ensure that risks associated with IT systems are managed to an acceptable level by securing the Operating Systems (OS) access.

User Authentication

All OS users shall be authenticated before providing access

All OS users shall have a unique user id.

Account Policy

9.5.1 OS shall enforce minimum password length.

OS shall enforce password expiry.

OS shall enforce password history.

OS shall enforce account lockout feature.

Non-essential user accounts shall be deleted.

8.10.3.Temporary user accounts should be deleted immediately

after use

New User Provisioning

All OS users shall be created only after approval from the department head / branch manager.

New user creation and user privilege granting shall not be done by the same person. Rather it will be done by two separate individuals.

User rights shall be allocated based on the principle of least

privilege. 9.7 Security of User Credentials

OS shall be configured to store user-id and passwords in a secure manner.

OS shall be configured to send user-id and passwords over the network in a

secure manner. 9.8. Logging

Logging shall be enabled in the OS to track all critical

activities

9.9 Non Essential Services

All application and OS services that are not essential for the functioning of the system shall be disabled.

Login Banner

OS shall have an initial login message configured stating that the system shall be used only for authorized activities.

Anti-Virus

9.11.1Anti-virus software shall be installed on all systems with risk of virus

infection.

9.11.2.Anti-virus software shall be updated with latest signature patterns.

Naming Conventions

Standard naming conventions shall be used while assigning host names at OS level to ensure easy identification and to prevent name clash.

Application owners are responsible for ensuring compliance with naming

conventions. 9.13. Documentation

All security settings of OS shall be documented in the Secure Configuration Document (SCD) and shall be approved by ISC.

Application owners shall get the relevant secure configuration documents from ISC and include thesettings as part of application installation/configuration document.

Review of User Access Rights

Users' access rights shall be reviewed on a periodic basis.

Emergency Procedures

Activities performed with privileged ids during emergency situations will be subjected to review and control.

10. Procedures for Application Security

Purpose

Applications are vulnerable to various, kind of attacks, which are exploited by a malicious activity. Computer software owned or licensed must not be copied by users, employees

and others for use at home or any other location. Exceptions to this will be specifically authorized by the Information Owner. Anyone could access information and/or data wherein security controls like authentication mechanism can be easily bypassed. Hence, it is imperative that Security controls to protect the application are appropriate and deployed on a continuous basis. .

Policy Statement

Application deployed in bank shall have controls for secure input processing, through system, storage and output of data. Application shall be tested for security performance before deployment & for high availability. Access to application shall be restricted to authorized persons & access will be provided on the principle of least privilege.

Scope

Application is required for design, development, configuration, integrating and testing of the software. Bank has to controls for secure input, processing, storage and output of data. Applications must be tested for security and performance before deployment and shall be managed for high availability. Access to application must be restricted to authorized persons and rights provided on the principle of least privilege.

10.4. Application Owner

Every application deployed in the bank shall have an application owner.

Application Access

Application shall authenticate all users/ other applications before allowing access.

Application shall ensure that all transactions have a separate requestor and approver.

There shall be provision for multiple privilege levels within the application.

All application users shall be created only after approval from business unit representative. All user access shall be provided based on the principle of least privilege.

New user creation and user privilege granting shall be done by separate persons.

All user-ids created shall be recorded and acknowledged in a User-ID register.

Application shall have an initial login message configured stating that the system shall be used only for authorized activities.

Application shall display the following information on completion of a successful log-on:

Date and time of the previous successful logon.

Any unsuccessful login attempts since the last successful logon.

User IDs shall not give any indication of the user’s privilege level.

Data Security

All data communication within the application and with other applications shall be secured.

Application shall store all sensitive information including login credentials and customer data in a secure manner.

Application shall have facility to check the integrity of data.

Application owner shall define the retention period for all data handled by the

application. 10.7. Input Controls

10.7.1 User inputs shall be checked by the application to ensure it is both appropriate and expected.

10.7.2. If the data is input through batch processes, adequate controls shall be implemented to prevent any errors.

Processing Controls

Application shall ensure correct sequencing of processes.

Application shall ensure that all pre-requisites are met before triggering a particular process.

Account Policy

Application shall enforce minimum password length.

Application shall enforce password expiry.

Application shall enforce account lockout feature.

Application shall enforce password history.

Application shall enforce password change for new user atfirst

login. 10.10 Database Access

Account used by the application for accessing the backend database shall have provision for password change.

Access rights shall be allocated based on principle of least privilege

Audit Trails

Application shall have the provision for logging all transactions. The transactions shall be traceable to associated user-id.

Application shall have the facility to log all security related events.

Application owner shall define the retention period for the log files based on the bank's data and log retention policy.

Error Handling

Application error messages shall not reveal any sensitive information regarding the application architecture or expected inputs.

Capacity Planning

Application owner shall identify the system requirements for deploying the application including software and hardware requirements.

Performance Testing

Application owner shall ensure that application is tested for peak load conditions before deployment.

Security Testing

Application owner shall ensure that the application is tested for security before deployment

Documentation

ISC is responsible for creating a secure configuration document for the application in consultation with the application owner.

Application owner shall ensure that detailed documentation is available for setup and maintenance of the application.

10.16.3 Adequate backups of all documentation shall be maintained.

11. Database

Purpose

Bank's database contains critical and confidential business information of its constituents which have to be protected at all times. Hence, it has to be ensured that database is configured to protect client information and at the same make them available to authorized users on authentication. The organization needs to define and develop adequate controls to secure its database.

Policy Statement

The technical team (IT department) shall implement database system configured as per best security practices. Adequate controls to maintain confidentiality, integrity and availability of database at all times shall be put in place. User access to database shall be

provided as per authorization and based on authentication. Database access will be given strictly based on business, operational needs and requirement.

File System Security

Operating systems files storing database information shall be secured against unauthorized uses. The Database systems store all information, configured and data in operating system files. Also these files are protected at OS level permissions.

Database administrator shall ensure that the appropriate permissions are on these files in the secure configuration documents for database.

Database Administrator shall ensure that these files are secured as per secure configuration document for database.

User Authentication

All database users shall be authenticated before providing access. Access shall be provided only after providing user-ID and password. No account can have with default or with no password.

All database users shall have a unique user-id, which shall not be shared. There will be no common user ID.

Database shall be protected against SQL-injection attacks. Validation shall be done both at the server as also at client.

New user provisioning

User accounts shall be created in the database only for application access, database backup and database maintenance activities.

All database users shall be created only after approval from the application owner / branch manager.

New user creation and user privilege granting shall be done by separate persons.

User rights shall be allocated based on the principle of least privilege.

Separate user IDs shall be allocated to the same user for performing privileged and normal (non-privileged) activities.

Account Policy

11.6.1 For database purposes administration shall enforce user account policy setting:
Database shall enforce minimum password length Database shall enforce password history
Account lockout feature shall be enabled
Password expiry shall be set as per policy, say 30 days

All vendor supplied default user IDs shall be renamed or disabled.

User-IDs shall not give any indication user's privilege level.

12. Patch Management

12.1. Purpose

The hardware having computers and applications should be frequently patched to protect against widespread worms, malicious code that target known vulnerabilities on non-patched systems, resulting in downtime & business impact on banks.

The downtime and business impact can be avoided by have effective patch management which will keep updated the IT system and applications deployed in the bank.

12.2 Policy Statement

The bank shall be secured against known vulnerabilities in operating systems and applications software through an effective Patch Management process.

12.3. Scope

The information assets like computers and applications should be frequently patched to protect against widespread worms, malicious code that target known vulnerabilities on non-patched systems, resulting in downtime & business impact of banks.

This has to be implemented to have effective patch management process in order to keep the IT system and application deployed in banks, updated and patches

12. 4. Identification & Validation of Patches

- Network administrators, database administrators and application administrators are responsible for identification and validation of all patch related issues concerning their domain of work. IS Officer (ISO) is responsible for identification and validation of all security related patches.
- To ensure that all patches are tracked, the respective administrators shall:
- Maintain an updated list of OS, application and database related patches released.
- Subscribe to the vendor's security patch mailing list or have agreements with vendors for receiving new security patches.
- The respective unit head shall validate if the released patch is applicable to the environment.
- If the patch is affecting a particular service and is not implemented administrators shall track and keep a record of the discarded patches for future audit purposes.

- Fill up the patch installation report whenever a new patch is identified.

Patch Classification.

- Patches shall be categorized into different criticality levels based on the threat to the systems. Bank shall analyse the applicability of the patch to the environment and determine its criticality.
- The following guidelines may be used to classify the criticality:
- High Criticality (Servers).
- Vendor has assigned high criticality.
- Vulnerability addressed by the patch can be exploited remotely.
- Publicly known worms or Trojans exploit the Vulnerability.
- If the assessment of the criticality of the patch to the Bank environment shows that the patch released does not fall under any of the above category, it is classified with low criticality.
- High criticality (Desktops):
- Vendor has assigned ‘high’ or ‘medium’ criticality.
- Vulnerability addressed by the patch can be exploited remotely.
- 12.5.8. If the assessment of the criticality of the patch to the bank’s environment shows that the patch released does not fall under the above category, it is classified with low criticality.
- 12.5.9 Respective administrators shall verify if the patch shall be applied on the respective systems.

Patch Scheduling & Prioritization.

- Patches shall be tested and applied on a priority basis based on their identified criticality.
- Plans shall be developed for standard patch releases and updates. Separate plan shall be developed for critical security and functionality related patches and updates.
- Patches shall be tested and applied in the following time frames:
- Critical: As soon as possible after release (installed immediately after testing).
- High: Within one day of release (installed during scheduled daily change control window).

- Medium: Within one week of release (during scheduled weekly change control window).

- Low: Within one month of release (during scheduled monthly change control window).

Patch Application Procedure.

Desktop Patches Application Procedure:

- Security Team shall check if the patch installation affects the operating system or application's functionality on a test desktop.

- If the tested patch is successful then it shall be applied on all the desktops using an automated solution.

Server Patch Application Procedure:

- Server monitoring team / application administrator shall check if the patch installation affects the operating system or application's functionality in a test server.
- If the tested patch is successful, it is applied on the production server manually, after an approval from the Head – IT Infrastructure is obtained through the change management process.

Patch Tracking.

- Implementation team shall submit the patch tracking sheet on a monthly basis to the respective unit managers.

- The respective unit managers shall be responsible for tracking the patches using the patch tracking document and reviewing it using the patch installation report.

- The IS team shall track all security patch implementations using the patch tracking document and review it using the patch installation report. This is to ensure that all patches which are not installed can be tracked for future reference.

Audit & Assessment.

The ISO/IS team shall review the installation of the security patches once in a year by carrying out a vulnerability assessment on all the desktops, laptops, servers, networking devices and security devices in a staggered manner.

Centralized Patch Management System.

- A centralized patch management system shall be in place to ensure patches are applied on desktops in a timely fashion.

- Applying patches to servers, applications, database and network devices can be done either manually or automated using the patch management system.

Enforcement

Compliance with the security policies will be a matter for periodic review by the ISO/ IS Team. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as deemed appropriate by the policies of management and Human Resources.

13. Back-up

13.1. Purpose.

Back-ups of essential information, data and software shall be taken on regular basis, one copy on site and one off-site. This should to be strictly followed to ensure that all essential information and SW could be recovered in the event of a disaster or failure of media. This would help to prevent loss of data which can impact in terms of delay, increased costs, loss of credibility & embarrassment.

Policy Statement.

Information system/asset owners (employees) shall ensure that adequate back-ups, as per stipulated periodicity are taken so that the data is not lost and can be recovered, in the event of an equipment failure, intentional destruction of data, or disaster. The IT department shall be responsible for operationalizing this policy.

Scope

There has to a mechanism of taking back-ups of essentials information, data and software. This shall be taken on regular basis, one copy on site and one off-site. This should to be followed to ensure that all essentials information and SW could be recovered following a disaster or failure of media. This would help to prevent loss of data which can impact in terms of delay, increased costs, loss of credibility & embarrassment.

Backup Process

- Backup shall be taken regularly to ensure that data can be recovered when required.

- The components which need to be backed up shall be defined for each application.

- Backup scheduling shall be done to ensure that all critical data is backed up without affecting system operations.

- Type and frequency of backup and type of backup media to be used shall be decided by the application owner taking into consideration the following parameters.

- Volume of transactions Criticality of data

- Recovery time constraints

- Time frames for retention of backup data shall be defined by the application owner.

- All backup media shall be properly labeled.

- Individual users shall be assigned roles and responsibilities for backup and recovery operations.

- Registers shall be maintained to track the backup and recovery operations.

Security of Backup Media

- Critical data on backup media shall be secured to prevent unauthorized access.
- For critical data, multiple copies of backup shall be maintained on different media.
- Backup shall be secured against environmental threats.
- For critical applications, a copy of the backup shall be stored offsite.
- Adequate security measures shall be taken while destroying the data

Migration of Backup Data

If there is a change in application software or backup media type, previously backed up data shall be converted to new format. However if this is not possible a backup of entire environment shall be taken as a set and kept for future reference and use.

Recovery Testing.

o Testing of recovery shall be done periodically.

p Frequency of recovery testing shall be determined by the application

owner. 13.8. Documentation.

Backup and recovery procedure documents shall be created and maintained by the application owner.

14. Personnel

14.1 Purpose.

People are the key assets in creating, storing, maintaining, distributing, processing and protecting the information/data of the organisation. All employees as also contractual users should adhere to all the IS security guidelines and access information purely based on job responsibilities and requirements. They should not access information for personal use. The access can be revoked or modified with changes in such responsibilities.

14. 2 Policy Statements.

People are the key assets in creating, storing, and maintaining, distributing, processing protecting. All employees as also contractual users shall adhere to the personnel security

and access based on job role and responsibilities. The access can be revoked or modified with changes in such job role and responsibilities.

Bank shall ensure that each employee is made aware of the importance of IS and their role in ensuring IS. Also employees will be instructed to strictly adhere to various IS related instructions and not to use information for other than official purposes. Employees will be informed of their access and other rights which can be revoked in the event of role changes.

Scope

- This policy covers all employees of the bank as also those of outsourced agencies and third parties.

- All employees with access to information systems of the bank must be aware of their responsibilities in protecting information systems under the security policy. Failure to adhere to IS responsibilities will entail appropriate disciplinary action. Access to information systems will be provided based on job responsibilities and revoked or modified with changes in such responsibilities.

Terms of Employment

o Appropriate verification checks needs to be carried out prior to hiring employees, contractors or temporary staff for computer related position of trust.

p Security clauses relevant to the employment shall be incorporated into employee's contract, which includes clauses on non-disclosure, confidentiality of information and acceptable usage of IT resources in the bank.

q All external entities like contractors, consultants or temporary workers, having access to information assets of the bank shall sign IS responsibilities and non-disclosure agreement documents.

Training and Awareness

All employees of the bank shall be provided with awareness on their security responsibilities as per the policies and procedures of the bank to enable them to protect bank's information assets.

All employees of the bank shall receive prompt notice of changes in security policies, including how these changes may affect them and how to obtain additional information.

Periodic security reminders shall be given to employees, agents and contractors, so that they are made aware of security concerns on an ongoing basis.

Compliance.

vi. Every Employee must agree to perform their security responsibilities and comply with the requirements specified in the security policies. Non-compliance with security policies can lead to disciplinary action.

vii. Employees should ensure that sensitive information should not be discussed in the presence of external personnel or other bank employees.

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

Certain categories of activities, which have potential to harm, or actually harms information assets of the bank are defined as security violations and are strictly prohibited. All security violations will entail disciplinary action as bank may deem fit.

Responding/reporting to Security Incidents: All employees have the responsibility to report suspected IS incidents and vulnerabilities as soon as possible to their controllers or directly to ISC through ISO.

Unless required by law to disclose security incidents, employees shall not report incidents to external entities except with the approval of appropriate authority. Any reporting to external entities shall be authorized by Head Office of IT after weighing the pros and cons of external disclosure.

Termination.

In the event that an employee, consultant or contractor is terminating his relationship with then Bank, the controller is responsible for –

Ensuring all property in the custody of the worker is returned. Notifying all administrators to terminate user accounts.

Terminating all other work related privileges.

15. Password

Purpose.

If an unauthorized user or a customer who is not authorised gains access to banks information and information assets, it could result into loss of confidence constituents and result in compromise with integrity of data.

Generally the user and customer gain access to information/data through user-ID and the password provided for securing transactions. Access to systems should be strictly limited for the genuine business purposes with the complement of User ID and password.

Policy Statement

Every user shall be assigned a unique user ID. Users both employees and customers shall choose/create their passwords in accordance with policy and shall protect at all times during its generation, delivery, storage and usage. The password change process shall be well calibrated. Users and Customers will be mandated to periodically change the password. Bank will educate the customer on the need for confidentiality in the password, not sharing it with others and the consequences of sharing the password.

15.3. Scope

This Scope includes all employees of the bank as also from the outsourced agencies and third parties personnel.

15.4 Construction of Passwords.

System Components shall specify the construction of complex passwords; for passwords to be termed as complex, they shall have at minimum, combination of the characteristics like alphabets (combination of capital and small letters), numerals and some special characters.

Password construction rules are applicable even if not currently enforceable by the platform/application and these rules shall be communicated to users.

Disabling Access

The account shall be locked out after five (*say* 5) failed password attempts.

Five (5) days prior to password expiry the user shall be alerted by a warning message to change the password on every login.

System and applications shall verify the user's old password before allowing the user to set a new password.

Generation of Password.

2 Passwords shall be encrypted when transmitted across any network

3 The display and printing of passwords must be masked using asterisks or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

4 Passwords must not be logged or captured.

5 A password must not be displayed on the data entry or display device.

6 Usage of group and shared passwords are prohibited.

7 Passwords must not be communicated via email if it is not encrypted for all internal employees.

8 Passwords shall never be written down or stored in an unprotected fashion (including mobile or similar devices) without encryption.

9 Passwords shall not contain whole or part of the user's account name.

15.6.9. Users shall not use the following type of passwords words found in a dictionary (English or foreign):

6. Names of family, pets, friends, co-workers, fantasy characters, etc.;
7. Computer terms and names, commands, sites, companies, hardware, software;
8. Words derived from organization name such as that of bank or any derivation;

9. Birthdays and other personal information such as addresses and phone numbers;

Resetting Passwords

The user shall submit request for password reset through a password reset form to IT service desk. IT service desk shall initiate the request password reset process.

IT Service desk shall carry out proper identity & verification check of the user before disseminating new password as per the password reset request.

"15.7.3. Remember Password" feature of applications shall not be used (e.g., web browsers, websites).

15.7.4. Users are encouraged to use passphrases. Encourage generation of strong passphrases

Customer Facing Applications

Customer facing applications shall be locked out after three (*say* 3) incorrect password attempts.

Accounts must be enabled only after being authorized by bank officer and the new password shall be mailed to bank customer's point of contact and his manager.

Login to all customer facing applications shall be by use of 2-factor authentication mechanisms. These days latest combination of user-ID, password with biometric authentication provides very good security.

Resetting of Default Passwords

Default passwords shall be reset immediately on first initialization by any system, network / infrastructure device or application and these must be moved into production only after all default passwords are changed.

Compliance to Password Policy

- ISO / IS team may conduct offline password cracking and online guessing testing for compliance monitoring on a periodic basis.
    - If a password is guessed or cracked during one of these scans, the user will be required to change it.

Systems for which passwords requirements cannot be enforced due to system limitations shall be documented with the ISO / IS team.

Disciplinary action may be taken against users found to be negligent in the use of passwords.

15.11. Enforcement

Compliance with the security policies will be a matter for random periodic review by the ISO/ IS team. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as deemed appropriate by the policies of management and Human Resources.

16. E-mail usage and security

Purpose.

The e-mail system for the bank is required for day-to-day function for genuine banking and operations. It is also a part of the customer service. A lot of internal information is shared with employees and functions/function heads through email. As such appropriate controls have to be provided for security for e-mail.

Policy Statement

E-mail ID and access shall be made available to employees purely based on business needs. Every employee shall develop a password for accessing the mail. Email activity shall be protected adequately to provide availability, exchange of information between employees of the bank and with the third parties. Bank will protect the system with appropriate technology and other means against breach or unauthorized access. Employees will not be allowed to use email for personal work.

Scope.

E-mail infrastructure consisting servers that host all e-mail application; desktops, mobile handsets have access to e-mail applications. Any other systems that Interfaces with e-mail system. Operating system and application that provide foundation for e-mail systems. Personnel under all departments responsible for administering and maintaining e-mail system.

16.4. E-mail Service – General

1.Email is a business communication tool and employees shall use this tool for the business in a responsible, effective and lawful manner. Users e-mail can be terminated or bank could take appropriate punitive action in case misuse of the e-mail system is discovered.

Users shall use the standard disclaimer approved by bank at the end of the e- mail.

All e-mails stored locally on the user's desktop shall be protected by password.

Users shall promptly report all suspected security vulnerabilities or problems that they notice with the e-mail system to the Central Email Team.

Bank has the authority to intercept or disclose, or assist in intercepting or disclosing, e-mail communications.

Use of bank's official mail account for personal purposes shall be discouraged.

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

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

The email message including all attached files shall be limited file size Personal email ID is not provided for the bank, shall not be used for official communication.

Confidential or sensitive messages or information shall not be transmitted over e- mail unless it is encrypted or password protected.

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

Account Protection

Users owning the email account are responsible for the content of email originated, replied or forwarded from another account inside outside the bank.

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

Users should exercise caution in providing their email account or other information to websites or any other internet for mailing list.

Server Monitoring

The system performance of e-mail servers shall be monitored on a periodic basis.

The logs of the e-mail application shall be monitored periodically to ensure proper functioning

Monitoring & Reporting

Bank reserves the rights to monitor the e-mails. Emails may be intercepted or disclosed or bank may assist in interception or disclosing email communication to ensure usage in terms of policies

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

Document and Storage Security

Central Email team shall maintain updated documents for installation, configuration and administration of email server and client.

Central Email team shall be responsible for distributing the relevant documents to branch system administrators.

Backup and Redundancy.

All documents containing sensitive information shall be marked as secret and /or confidential both in electronic and in paper form.

All removable media including CD and/or DAT tape shall be labelled as secret or confidential if it is used for store sensitive documents .

Confidential document and media shall not be left unattended.

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

Un-used documents, paper shall be destroyed using shredder machine.

Users should keep a backup copy of important documents.

Backup of the e-mail server shall be taken on adaily basis.

Test recovery of backup shall be done on a periodic basis.

There shall be standby server for critical e-mail servers.

16.10 Change Management

7.10.3.Any changes regarding the e-mail application shall follow change control policies.

16.10.2. The Central Email team shall be responsible for implementing any changes to the e-mail server.

17. Change Management

Purpose

Unauthorized changes and ad-hoc changes in the IT and other electronic systems could lead to system getting interrupted and result in genuine persons and users unable to access system or information assets. It is laid down that major or minor changes to any information assets where ever necessary should be carried out with prior approvals. The changes are to be identified and monitored. The entire process will have to be documented. It is provided that changes will be implemented in test environment before taking to production.

Policy Statement

Changes to the IT systems shall be performed in controlled manner. To ensure that the risk associated with changes are managed to an acceptable level, changes will be made only after careful consideration of its need, impact and proposed changes will be thoroughly tested before these are deployed.

Scope

This applies to all critical IT assets as also applicable to the personnel carrying for approval, administering & maintaining, tracking changes. Applies to business and/or application owners for smooth functioning.

Change Request and Approval.

All business applications shall have a change control team (called the Team) for approving and tracking critical changes.

The Team shall identify all changes related to the application that require approval before implementation. All changes that have an impact on the security level and functionality of the application shall be approved by Team.

When a user/system administrator requires a critical change to be made, a formal change request shall be made to the Team. The change request shall contain of the following details:

Change objective
Description of the change
Any alternate solutions

Team shall take a decision on whether to proceed with the change request based on the following parameters:

Need for change
Impact of change
Priority of change
Security implication

If the change request is approved, the team that will be involved in implementing the change to prepare a detailed implementation plan. The implementation plan document shall contain the following details:

Time and resource requirements

Pre-requisites (if any)

Implementation steps
Downtime requirements
Test plan
Roll back plan.

17.5. Testing of Implementation Plan

The team responsible for implementation shall make the change on a test system as per implementation plan and confirm functionality.

17.6 Implementation of Change

The team responsible for implementation shall perform the changes on the production system in accordance with the implementation plan.

The team responsible for implementation shall submit a post-implementation report containing details of actual steps done during implementation.

The application owner shall certify that only changes authorized by the change control committee have been done.

Minor/Emergency Changes

Minor/emergency changes need not seek the approval from team.

The persons responsible for implementing the change shall submit a post implementation report to the Team.

Review of Change

Team shall evaluate the effectiveness of change based on the following parameters.

- Changes achieving the desired objective
- Adherence to implementation plan

Team shall ensure that ineffective changes are rolled back.

Application owner is responsible for maintaining all documents related to change management for future reference and audit purposes.

18. Monitoring

Purpose.

IT infrastructure components form a crucial part of assets of the banks. IT assets are constantly under threat from hackers and other malicious users and as a result needs to be monitored effectively on a continuous basis for identifying any abnormal activities and for the purpose of protecting the asset. The effectiveness and applicability of IS controls have to be monitored based on control testing criteria, purpose of testing and results periodically reported to the management. Security controls need to be continuously implemented on IT assets to protect them from unforeseen threats.

Policy Statement

The bank shall establish an effective enterprise level system to centrally monitor IS controls. All access to critical applications and banks network shall be monitored for suspicious activities or security breaches. Adequate response mechanism shall be set up for controlling security breach, if any.

Scope

All access to critical applications and the bank’s network shall be monitored for suspicious activities or security breaches and adequate response mechanism shall be setup for controlling security breaches.

Security Monitoring

All access to critical systems shall be monitored continuously for tracking security threats. Network based Intrusion Detection Systems (IDS) shall be setup to monitor access to critical systems including the following.

- Systems accessed by external networks.
- Critical internal application servers.

Host based IDS systems shall be deployed on critical systems which cannot be monitored through network based IDS.

The attack signatures enabled on the IDS system shall be classified based on the criticality. Appropriate alerts shall be configured for each category of attacks.

Central Monitoring Team (CMT) shall ensure that latest attack signatures are updated on the IDS systems.

CMT shall be responsible for tracking the IDS alerts.

CMT shall submit periodic reports on attacks detected by the IDS systems to the Product Manager - Information Systems Security Formulation and Implementation Team (ISC) and respective application owners.

All critical systems shall be monitored for uptime by respective application owners.

18.5. Performance Monitoring.

Application owners are responsible for setting up automated systems for monitoring the performance of critical servers and devices.

Application owner shall define acceptable usage levels for all parameters that are being monitored.

In case of all critical applications, systems shall have a well defined service level agreement. This agreement shall define all the performance parameters to be monitored.

18.6 Log Monitoring

Logging shall be enabled on all critical devices including application servers, database and network devices.

Application owner is responsible for setting up the process for log analysis and reporting.

Application owner shall ensure separation of roles between the person(s) undertaking log review and those whose activities are being logged.

Performance monitoring systems shall have provision for automatic alerting.

19. Outsourcing/Third Party

Purpose

There are a number of IT based activities that the bank has outsourced. These include AMC for hardware and software, maintaining ATM etc. The bank is aware of the risk of improper access to information and information assets from users of third party or outsourcing agencies which could prove detrimental to banks interests. A risk assessment exercise should be carried out to determine the specific security requirements in such cases. Contract with third parties or outsourcing agencies should be established with necessary security conditions and service levels in mind.

Policy Statement

Banks shall ensure that access to the data processing facilities and intellectual property

rights of the bank are well protected from third party service provider's entities and controls by taking adequate measures.

Scope

Risk of improper access from users of third party or outsourcing agencies may be exposed to banks. A risk assessment should be carried out to determine the specific security requirements in such cases. Contract with third parties or outsourcing agencies should be established for necessary security conditions & service levels. Contractual requires in a risk management strategy.

A detailed feasibility study shall be conducted by Head Office IT department prior to outsourcing to determine the need, benefit and risks of outsourcing.

19.3.4. The feasibility study shall evaluate the outsourcing requirement along the following parameters:

Cost benefit

In-house capabilities

Strategic advantage

Risks in terms of vendor meeting performance requirements, security standards and regulatory compliance.

Outsourcing Plan

Head Office IT will create an outsourcing plan after the feasibility of outsourcing is established. The outsourcing plan will include the following details:

Key objectives and requirements in terms of quality of service, cost and deliverables Time frame for outsourcing

Transition plans

Key risks to be addressed and mitigated in outsourcing activities

Vendor Selection

Vendor evaluation and selection will be as per the procurement policy of the bank. Vendor's reliability in delivery of service, stability of operation and flexibility to meet bank's needs are important consideration in outsourcing apart from expertise and experience of the vendor.

Bank can conduct an audit of operational & security controls of the vendor prior to final selection to ascertain that all risks identified in outsourcing plan can be mitigated by the vendor.

Transition Risks.

Transition of services from outsourced vendor to bank or vice-versa will be as per a transition plan and clear responsibility will be assigned within bank fortransitioning.

The following needs to be considered when operations are being transitioned from the outsourced vendor to bank or vice-versa:

Knowledge transfer, including skills, process methodologies & documentation
Transfer of bank data and documents, transfer of any ownership of assets from vendor to bank

Assigning and revoking access rights, logical and physical, over the IT assets of bank Support requirements post transition

Security

ISC will be advised of the decision to outsource and details of the solution and the vendor. ISC will communicate to the vendor the requirements under the IS policies of the bank, relevant to the activity being outsourced and ensure its compliance by the vendor.

Bank shall retain the right to audit the vendor for its compliance to security requirements of bank.

Bank shall ensure that vendor meets all legal requirements, including pertaining to the functions undertaken on behalf of bank.

Bank shall ensure that the outsourced vendor has adequate contingency plans including backup & recovery, redundancies, disaster recovery and insurance coverage to meet the service levels.

In the case of software development outsourcing adequate measures including software escrow and software code ownership shall be considered to ensure that source code is available in the event of vendor failure.

For software development outsourcing, the application shall meet the security requirements defined in application security policy.

Bank shall make fallback arrangements commensurate to the criticality of outsourced activity and risk of its failure.

Data ownership shall be retained by bank when business processes are outsourced.

Performance.

The contract with vendor will include the Service Level Agreements (SLAs) as defined in the Procurement Policies.

The SLAs shall be monitored and managed by the IT department.

For software development outsourcing, delivery checks for functionality, security performance and documentation shall be carried out before software acceptance.

Contractual Terms.

The contract for outsourcing between the bank and the outsourced vendor shall

cover the following.

Service levels, roles & responsibilities of vendor, obligations of bank, timeframe, cost of service and penalties / reward for performance.

Requirements for complying with security policies, intellectual property rights and right of bank to audit the vendor.

Requirements during transition to be adhered by the outsourced vendor.

Disaster recovery provisions, data ownership and software escrow provisions.

Problem resolutions, change control, contract re-evaluation and termination

THE **OUTSOURCING POLICY SHALL BE IN CONFORMITY WITH THE GUIDELINES ISSUED BY RBI FOR OUTSOURCING BY BANKS.**

20. Business Continuity

Purpose

To fulfil 'the banks' commitment to protect its customers and in the interest of rendering uninterrupted banking services it would be prudent for the Bank to thwart all kinds of threats to its business which could have the potential to disrupt its operations. In other words bank should ensure robust systems such that its business continuity is not threatened. In view of this, critical information systems of the bank should be planned and suitably designed to ensure continuity of operations, even in the event of a disaster. IS is one such critical aspect. IS will help counter interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Policy Statement

Bank shall ensure the safeguard of its information and information assets to minimize the risk, costs & duration of disruption to business operations. Bank will establish and maintain integration between response plans, Disaster Recovery Plan (DRP) & BCP. Bank will have a plan for effective Continuity of Business & a well rehearsed recovery process or a combination of these which will enable the resumption of critical business activities.

Scope

The Business Continuity and Disaster Recovery policy would be made applicable to all branches of the bank, and all departments at administrative and head office of the bank. It would encompass all information systems critical to the business operations of the bank covering all employees as also the critical functions outsourced and managed by third party vendors.

Information systems that are critical to the bank's business shall be planned for continuity of operations in the event of disasters. A written DRP shall be maintained, tested and updated for such systems. The plan shall provide for appropriate safeguards to

Minimize the risk, cost, and duration of disruption to business processes caused by disasters.

DR Requirement

All centralized applications with bank -wide / State wide deployment shall have a

DRP.

Bank will develop a common DR plan.

Business Impact Analysis

Bank will setup a DRP team.

DRP team shall conduct a Business Impact Analysis (BIA) to understand the critical IT functions and the acceptable downtime.

Disaster Recovery Strategy (DRS)

DRP team shall evaluate different recovery strategies based on the results of the BIA.

DRP team shall present the possible recovery strategies and requirements to the business unit head.

Disaster Recovery (DR) Plan

Disaster recovery plan shall be developed based on the strategy.

DRP team shall identify the conditions under which the DRP shall be

activated. 20.8. Awareness and Training Program.

Awareness and training program shall be conducted to educate the users about the DR plan

DRP team shall decide on the frequency and mode of training.

Testing of DR Plan

Test exercise shall be conducted to verify the DR plan.

DRP team shall decide the frequency and mode of testing.
The DR plan shall be reviewed and corrected based on the test results.

Review of DR Plan

The head of IT shall be responsible for ensuring that the DR plan is updated and meets business objectives.

20.11. Maintenance of Emergency Contact Numbers.

A detailed list of contact numbers of the following entities shall be maintained and made available at all locations of the Bank having information assets.

EMERGENCY CONTACT NUMBERS

S.No.	Department/Office	Telephone Number	Mobile/Alternate No.
1.	Police		
2.	Fire Brigade		
3.	Hospital		
4.	Ambulance		
1.	Power/Electric Supply		
2.	UPS Maintenance		
3.	Batteries Maintenance		
4.	IT Hardware Maintenance		
5.	Application Maintenance		
1.	BCP Team Leader		
2.	BCP Team Members		
1.	IT Department Head		

21. ATM

Purpose

The objective of this policy is to prevent misuse and minimize security risks to ATMs installed in the bank premises and at off-site locations. The ATMs being an important delivery channel offering financial and non-financial services, the security risks must be considered on top priority for prevention of frauds.

Policy**:**

A network of ATMs exists in the bank where a secret ATM operation code will be issued to the customer in the form of Personal Identification Number i.e. PIN for ATM operations.

The concept of PIN prevents an unauthorized user from gaining access to the ATM network as a combination of physical card and PIN number is required for accessing the account for withdrawal of cash and/ or any other services offered by bank through card and ATM. ATMs will also be guarded suitably against theft, unauthorized access etc.

Scope**:**

This policy applies to all ATMs installed in the bank premises and at off-site locations.

Physical Security of ATM

ATM location and position should be as per specifications provided by Services department. (The ATM should be housed within the premises well away from perimeter glazing, particularly shop fronts, preferably directly against a strongly built internal or perimeter wall, which does not have vehicular access to its external face, and positioned to avoid a direct line of access from a door or other access point. To reduce the risk of vandalism to the ATM and to increase user safety, the ATM should be positioned in a highly visible and well-lit area that allows maximum surveillance by counter staff and other customers. Entrance / Exit should have a roller shutter with Central Lock, wherever possible, access lock be installed and operational. Walls of ATM enclosure should be double brick walls along with standard quality of strong roof minimum 4" thick (RCC) and standard flooring).

21.4.2 Access lock should be installed and operational so that the glass door fixed on

ATM entrance should open only when ATM Card is swapped / dipped by customer.

CCTV (Close Circuit Television) system shall be installed, and the circuit may be extended to ATM enclosure by fixing one camera in such a position from where face of customer and cash dispensation operations only can be captured for the better security control. In no case the camera should be directed towards ATM keypad to ensure that the keypad operations are captured.

The policy guidelines of Security Deptt. H.O shall be followed on deployment of security guards, fire detection system, alarm system, and CCTV surrendering system at the ATM site.

UPS, A/C should be maintained properly for trouble free operation of ATM.

Automatic fire detection, fire suppression systems and equipment in compliance with requirement specified by the Department of Fire Control or any other agencies of the Central or State Government shall be installed at the operational site.

General Security

The branch incumbents of Branches having onsite ATMs & officials of IT Nodal Centres during their Surprise inspection should thoroughly scrutinize ATMs frequently for preventing skimming and cloning of Cards. In case some suspicious device or activity is noticed by them at the site, the same should be reported immediately to Hardware vendor for proper inspection.

Physical and logical access control of ATM, Network elements, hardware, ATMs, HSM &card operations shall be followed meticulously.

PIN security, authentication guidelines as issued by VISA, NPCI, RBI from time to time shall be strictly implemented and complied with.

Wherever CCTV is installed in ATM cabin, Cash replenishment or Cash Removal in ATMs should be done under the CCTV surveillance system (if deployed) with the premises locked and customers excluded.

In order to ensure security of the cash the ATM Safe / Chest is provided with either one lock (primary lock) or two locks (a primary and a secondary lock). In case of single force Primary combination lock may be provided with the physical key.

ATM Chest operations activity shall be assigned to two custodians. Moreover following guidelines with respect to the operation of combination locks of ATM must be adhered.

The combination number / password for the combination locks should always set and re-set by the respective custodians.

The combination number/ password must not be disclosed to anybody and the secrecy of the same must be maintained strictly. Whenever the combination number / password is set / reset, the combination lock must always be checked by opening and closing the lock using the new combination number without closing the door of the Chest / safe. Once the new combination number / password is successfully tested as per point-2 for each lock, the Safe / chest door must be closed and locked. After setting the combination number /password, same must be noted on a piece of paper and kept in the sealed envelope.

The sealed envelope pertaining to the primary combination lock must be kept under the custody with Cashier and the sealed envelope pertaining to the secondary combination lock must be kept under the custody of branch incumbent, in case of bank custodian. The combination number / password of the lock must be changed periodically by respective custodians and it must always be changed in the event of change of duties / transfer of any custodian.

21.5.10 Whenever the ATM Chest operation is assigned to another officer/personnel, the combination number / password of the respective locks must be got set by the officials / custodians whom the job is assigned.

In case the ATM Safe / Chest has got only one combination lock with physical key as well then one custodian shall hold the physical key of the combination lock and second custodian shall have the combination password / number.

In case the password of a combination lock is forgotten or applied wrongly the sealed envelope of the same lock needs to be opened and the password stored in sealed envelope shall be used for opening the combination lock in presence of 2 officials of branch/ regional office/ IT Nodal centre, in all cases where bank officers are custodians of ATMs.

21.5.13 All the events viz. ATM safe operations, changes of password of combination

lock, access to the sealed envelope etc. must be recorded and authenticated by the officials and in whose presence the sealed envelope is opened.

In case of electronic lock, this must be ensured on time to time from the ATM vendor that the battery of the lock is charged.

Issue of personalized ATM Card & Pin Mailer

The personalized ATM cards and PINs should be kept in the custody of different officials.

All account where such cards are being issued should be marked in the same register wherein account no. should also be mentioned.

The returned/undelivered card/PIN mailer should be handled as per the prescribed guidelines as these are a vulnerable source of fraud.

The returned / captured card in ATM should be handled as per the guidelines of the bank and proper entries to be made in the register.

Confidentiality and security of information/ data be ensured as per the policy of bank and RBI guidelines

Loss and Theft of card

Upon receipt of information of loss/ theft of ATM card, the facilities against the card should be immediately frozen so that no transaction against this card should take place. Also ATM should be programmed to capture such lost cards on any attempt to use the same.

Different PIN should be allotted for the duplicated card. Old card must be made invalid before issuance of duplicate card.

Surrendered card should be marked as closed in the database using online software. Moreover, the same should be destroyed in the presence of two officials, recorded in the register.

ATM Network Security

The ATM network shall support recovery from successful and attempted breaches on security.

The ATM network shall support capabilities to ensure that users are prevented from gaining access to information or resources they are not authorized toaccess.

The ATM network shall support the capability to keep stored and communicated data confidential.

The ATM network shall support the capability that an entity cannot deny the responsibility for any of its performed actions as well as their effects.

The ATM network shall support the capability to retrieve information about security activities stored in the Network Elements with the possibility of tracing this information to individuals or entities.

The ATM network shall support the capability to generate alarm notifications about certain adjustable and selective security related events.

The ATM network shall support the capability to analyse and exploit logged data on security relevant events in order to check them on violations of system and network security.

Confidentiality

The ATM network elements should support confidentiality of communications, passwords and key material, configuration files, audit information, storage of active and inactive passwords and key material and addressing information between them.

Data Integrity

The ATM network elements should support integrity for communications, configuration files and audit information between them.

Key Management

The ATM network elements should support a key management system for the secure distribution of key encryption keys that are shared, and perfect forward secrecy for all confidential communications between them.

Authentication

The ATM network elements should authenticate all communications between them and support the capability to mutually establish and verify the claimed identity of the other entity.

If 'Online Card Not Present (CNP) transactions' are allowed through ATM- cum Debit Card, additional authentication / validation based on information not visible on the card shall be carried out and for all CNP transactions 'online alerts' to the card holder shall be sent involving usage of cards of various channels.

Non-Repudiation

The ATM Network Elements should protect against any attempt by a message originator to deny sending a specific message, protect against any attempt by a message recipient to deny receiving a specific message and protect against any attempt by one party to deny that an authentication or session establishment protocol was run between two parties.

Access Control

Entry to ATM room, server room, HSM, card management units etc. should be

specially authorized and restricted for others.

21.14.2 The ATM network element shall support the capability to limit the actions of an operator based upon the operator's identity.

Security

The ATM network element shall support the capability to limit an operator's privileges based on the method of access.

Audit

The ATM Network Element shall be capable of recording a set of events that is Specifiable by a Network Administrator.

The ATM network element shall be capable of recording the system time at which each audited event occurred.

The ATM network element shall be capable of recording the identity of the network Administrator who performed each action.

Activity Reporting

The ATM network element shall be capable of reporting events selected by a Network Administrator to the Network Management System as they occur in real time.

21.8. Security Recovery

The ATM Network Element shall support recovery from incidents that impede or degrade the performance of the ATM network element.

AADHAAR ACT,REGULATIONS & SPECIFICATIONS

The security aspects of Aadhaar, as defined by the Aadhaar Act regulations, primarily focus on robust data encryption, strict access controls, logging all authentication attempts, prohibiting sharing of sensitive information without consent, and employing strong biometric authentication methods, ensuring that only minimal personal data is stored within the UIDAI database, and implementing penalties for security breaches by authorized entities accessing the system.

Key security features of Aadhaar:

- **Data Encryption:**

All biometric data collected for Aadhaar is encrypted at the point of capture and stored in an encrypted format within the UIDAI database.

- **Limited Data Storage:**

The UIDAI system only stores minimal personal information like name, address, date of birth, gender, and biometric data, not linking it to other databases.

- **Authentication Methods:**

Aadhaar authentication uses a combination of biometric data (fingerprints or iris scans) and a one-time password (OTP) sent to the registered mobile number for added security.

- **Access Control:**

Only authorized entities, called "Requesting Entities" (REs), can access the Aadhaar database for authentication purposes, and they must comply with strict regulations regarding data usage and security.

- **Consent Mechanism:**

Any entity seeking to verify an Aadhaar number must obtain explicit consent from the Aadhaar holder before performing authentication.

- **Consent Form:**
  If our bank is using the the AAdhar number of any customer,where there is an approval required by a customer for which purpose the aadhar number is going to use.Example:-
  1) NON Transactional purpose(as KYC)
  2) Mappping IT AS NPCI to enable the customer to receive Direct Benefit Transfer(DBT) from GOI
  3) Changing the mapping at NPCI from one bank to another bank
  4) Availing AEPS and other services based on Aadhaar authentication.

Key regulations related to Aadhaar security:

- **Logging and Auditing:**

  All authentication attempts are logged, enabling tracking and monitoring of access to Aadhaar data.

- **Secure Device Standards:**

  Biometric devices used for Aadhaar capture must comply with specified security standards set by UIDAI.

- **Virtual ID (VID):**
  To further protect privacy, users can opt to use a Virtual ID for authentication instead of their full Aadhaar number. The First 8digits of Aadhaar number of customer should be masked.(Example- XXXX XXXX 5555)

- **Aadhaar (Authentication) Regulations, 2016:**

  Defines the processes for Aadhaar authentication, including biometric and OTP-based verification, and specifies the obligations of REs.

- **Aadhaar (Data Security) Regulations, 2016:**

  Outlines the security standards that must be followed by all entities handling Aadhaar data, including data encryption and access controls.

- **Aadhaar (Sharing of Information) Regulations, 2016:**
  Sets rules regarding who can access Aadhaar data and for what purposes, requiring explicit consent from the Aadhaar holder.
  Important points to remember:

- **Do not share your Aadhaar number openly:** Always use a Virtual ID when sharing your Aadhaar number.
- **Be cautious about providing your biometric data:** Only provide your biometrics to authorized entities.
- **Report any suspicious activity:** If you suspect any misuse of your Aadhaar data, report it to UIDAI immediately.