

Information Technology & Information Security Policy

Resolved and approved by Management Committee on Dated- 10.01.2025



THE UNITED PURI-NIMAPARA CENTRAL COOPERATIVE BANK LTD, PURI

HEAD OFFICE: KACHERI ROAD, PURI-752001, DIST: PURI (ODISHA)

CONTENTS

SL. NO.	TOPICS	PAGE NO.
	INFORMATION TECHNOLOGY POLICY	
PART-I A		
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.	Definitions: 8.1 Policy	4
9.	Information Technology/ Technology Risk	6
10.	IT Security and Controls in the Bank	7
11.	Information Security Policy: Objectives	7
11.2.	Scope of the IS Policy	8
12.	Owners and Custodians	11
13.	Responsibility of Board of Directors	11
14.	Steering Committee/ Information Security Committee	12
15.	Chief Information Security Officer (CISO)	12
16.	Coverage of the Policy	13
17.	To Achieve the Objectives	13
18.	IS Review	13
19.	Applicability and Exceptions	14
PART II – INFORMATION SYSTEMS SECURITY POLICY		
1.	Policies and Procedures	14
2.	Environment and Physical Security Policy	14
	2.1 Purpose	14
	2.2 Policy Statement	14
	2.3 Procedures: Scope	14
	2.4 Access Control	15
	2.5 Environmental Protection	15
	2.6 Data Centre Security	15
	2.7 Identification of Devices	15
	2.8 CCTV Monitoring	16
	2.9 Power at the Data Centre	16
	2.10 Fire Prevention and Control	16
	2.11 Environmental Safeguards	16
	2.12 Preventive Maintenance	17

	2.13 Monitoring	17
	2.14 Document Security	17
	2.15 Enforcement	17

3.	Acceptable Usage Security	17
	3.1 Purpose	17
	3.2 Policy Statement	17
	3.3 Scope	18
	3.4 Desktop Users	18
	3.5 Laptop Users	18
	3.6 Password Security	20
	3.7 Internet Usage	20
	3.8. Clear Desk	20
4.	Incident Management	21
	4.1. Purpose	21
	4.2. Policy Statement	21
	4.3 Scope	21
	4.4 Incident Identification	22
	4.5 Incident Reporting	22
	4.6. Incident Verification	23
	4.7 Incident Recovery	23
	4.8 Incident Prevention	23
	4.9 Incidents to UIDAI, CERT-in, or DPDPA	23
	4.10. Incident Reporting Procedure	24
	4.11. Root Cause Analysis (RCA)	25
	4.12 Corrective and Preventive Measures	25
	4.13 Post-Incident Review	25
	4.14 Continuous Improvement	26
	4.15 Latest Incident Reporting Template	26
	4.16. Conclusion	27
5.	Asset Classification & Handling	28
	5.1 Purpose	28
	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	30
	6.1 Purpose	30
	6.2 Policy Statement	30
	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	31
	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	32
	6.11 Enforcement	32
7.	Anti- Virus	32
	7.1 Purpose	32
	7.2 Policy Statement	32
	7.3. Scope	32
	7.4 Installation	33
	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	34
	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
	8.6 WAN access on bank's network	36
	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	39
	10.1 Purpose	39
	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	41
	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	42
	11.3 File System Security	42
	11.4 User Authentication	42
	11.5 New User Provisioning	42
	11.6 Account Policy	42

12.	Patch Management 12.1 Purpose 12.2 Policy Statement 12.3 Scope 12.4 Identification & Validation of Patches 12.5 Patch Classification 12.6 Patch Scheduling & Prioritization 12.7 Patch Application Procedure 12.8 Patch Tracking 12.9 Audit & Assessment 12.10 Centralized Patch Management System 12.11 Enforcement	43 43 43 43 43 44 44 45 45 45 45 46
13.	Back-up 13.1 Purpose 13.2 Policy Statement 13.3 Scope 13.4 Backup Process 13.5 Security of Backup Media 13.6 Migration of Backup Data 13.7 Recovery Testing 13.8 Documentation	46 46 46 46 46 47 47 47 47
14.	Personnel 14.1 Purpose 14.2 Policy Statement 14.3 Scope 14.4 Terms of Employment 14.5 Training and Awareness 14.6 Compliance 14.7 Termination	47 47 48 48 48 48 49 49
15.	Password 15.1 Purpose 15.2 Policy Statement 15.3 Scope 15.4 Construction of Passwords 15.5 Disabling Access 15.6 Generation of Password 15.7 Resetting Passwords 15.8 Customer Facing Applications 15.9 Resetting of Default Passwords 15.10 Compliance to Password Policy 15.11 Enforcement	49 49 49 50 50 50 50 51 51 51 51 52

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	56
	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	57
	18.4 Security Monitoring	57
	18.5 Performance Monitoring	57
	18.6 Log Monitoring	57
19.	Outsourcing / Third Party	58
	19.1 Purpose	58
	19.2 Policy Statement	58
	19.3. Scope	58
	19.4 Outsourcing Plan	58
	19.5 Vendor Selection	59
	19.6 Transition Risks	59
	19.7 Security	59
	19.8 Performance	60
	19.9 Contractual Terms	60
	19.10 Third Party Access	60
20.	Business Continuity	60
	20.1 Purpose	60
	20.2 Policy Statement	61
	20.3 Scope	61
	20.4 DR Requirement	61
	20.5 Business Impact Analysis	61
	20.6 Disaster Recovery Strategy (DRS)	61
	20.7 Disaster Recovery (DR) Plan	61
	20.8 Awareness and Training Program	62
	20.9 Testing of DR Plan	62
	20.10 Review of DR Plan	62

21.	ATM	62
	21.1 Purpose	62
	21.2 Policy	62
	21.3 Scope	62
	21.4 Physical Security	62
	21.5 General Security	63
	21.6 Issue of Personalized ATM Card & Pin Mailer	64
	21.7 Loss and Theft of Card	65
	21.8 ATM Network Security	65
	21.9 Confidentiality	65
	21.10 Data Integrity	65
	21.11 Key Management	65
	21.12 Authentication	66
	21.13 Non-Repudiation	66
	21.14 Access Control	66
	21.15 Security	66
	21.16 Audit	66
	21.17 Activity Reporting	66
	21.18 Security Recovery	66

DATA PRIVACY OF BENEFICIARY AADHAR HOLDER

1	Terms and Definition	67
2	Introduction	71
3	Purpose	72
4	Applicability	72
5	Personal Data collection	72
6	Specific purpose for collection of Personal data	72
7	Notice / Disclosure of Information to Aadhaar number holder	73
8	Obtaining Consent	73
9	Processing of Personal data	74
10	Retention of Personal Data	74
11	Sharing of Personal data	74
12	Data Security	74
13	Data Protection	76
14	Rights of the Aadhaar Number Holder	81
15	Aadhaar Number Holder Access request	81
16	Privacy by Design	82
17	Governance and Accountability Obligations	82
18	Transfer of Identity information outside India is prohibited	83
19	Grievance Redressal Mechanism	83
20	Responsibility for implementation and enforcement of the policy	84
21	Relevant Provisions of Aadhaar Act and Supreme court judgement	84
22	Contact Details	84