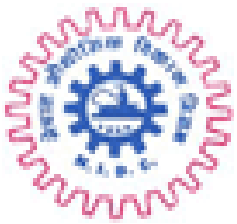


Nepal Industrial Development Corporation, NIDC

Durbar Marg, Kathmandu, Nepal.

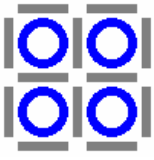
Information and Communication Technology Policy

(Including Disaster Recovery Plan)

NIDC - ICT Policy 2009

November 2009

Submitted by:



IT Professional Forum

Table of Contents

1. General 4
1.1. Introduction 4
1.2. Objective 4
1.3. Scope 4

2. Information & Communication Technology Infrastructure 6
2.1 Connectivity and Redundancy Connectivity 6
2.2 Network 6
2.3 Workstation 8
2.4 Antivirus Guidelines 9

3. Information & Communication Technology Ethics 10
3.1 User Profile Report 10
3.2 Password 11
3.3 Internet Usages 12
3.4 Prohibited Usages of Internet 13

4. ICT Security 14
4.1 Physical Access 14
4.2 Gateway to IT Branch 15
4.3 Email 15
4.4 Scope 16
4.5 Policy Definitions 16
4.6 Policy Provisions 16
4.7 Data Security 17
4.8 Power Equipment/Accessories 18
4.9 Hardware Standards 18
4.10 Software Standard 18
4.11 USB Drives 18
4.12 Magnetic Tape Drive 19
4.13 DVD/CD ROM Drives 19
4.14 Data Storage Policy 19
4.15 Cold Room for Servers 20
4.16 Power Cabling 20
4.17 Physical Protection 21

5. ICT Disaster Recovery Plan 22
5.1 Introduction 22
5.2 Disaster Preparedness 23
5.3 Disaster Recovery Processes and Procedures 23
5.4 Disaster Recovery Teams 25
5.5 Possible Risks, its Prevention and Recovery Plan 27
5.6 Disaster Recovery 28

6. ICT Policy Review and Monitoring 29
6.1 ICT Steering Committee (ICT-SC) 29

Appendix

Appendix A - List of critical documents stored in fire resistant vault

Appendix B - List of Original CDs/diskettes in fire resistant vault

Appendix C - List of IT Branch held documents stored in fire resistant vault

Appendix D - List of software manuals kept in fire resistant vault

Appendix E - Team Members and Contact Information

Appendix F - Grab List

Appendix G - Equipment in Cold Room

Appendix H - Vendor Contact List

Appendix I - Vital Computer Stationary Stocks

1. General

1.1. Introduction

Nepal Industrial Development Corporation (NIDC) is committed to maintain its Information and Communication Technologies (ICT) Systems secured and authenticated while providing its services, using ICT systems and doing business processes. Unauthorized use of ICT System of NIDC needs to be avoided and its system needs to be protected. The system is to be used only for official purposes of NIDC. Authorized use of ICT system is a team effort and related person must be aware of the provisions incorporated in this policy document. Users should be aware that the data that they create on the system remains the property of NIDC. Any information that users consider sensitive or vulnerable must be encrypted. Under this policy authorized individuals within NIDC may monitor equipment, systems and network traffic at any time for security and network maintenance purpose. Internal audit shall audit networks and systems on a periodic basis to ensure compliance as per this policy.

This document constitutes NIDC's policy for the management of ICT resources owned and administered by NIDC. The policy outlines the privileges and responsibilities of the staffs and also sets standards for the resources to be used.

Because of the difference in the operational capacity and availability of resources in branches, some of the specific items in this policy may not apply or be practical to branches. In such case(s), the General Manager may recommend the required amendment in the policies for Board of Director's (BOD) approval. Any permanent changes, to these policies shall only be effective upon the approval of the BOD.

1.2. Objective

The purpose of this Information and Communication Technology (ICT) Policy is to provide staff guidelines covering all aspects of ICT of NIDC. This policy outlines acceptable use of computer and communication equipment, software and hardware of NIDC and to prevent unauthorized use. The policy is prepared to prevent the occurrence of inappropriate, unethical, or unlawful behavior by any of the user of its computing systems and telecommunications networks. The policy also covers disaster recovery plan.

1.3. Scope

This policy applies to all stakeholders of NIDC. It is the responsibility of all operating units to ensure that these policies are clearly communicated, understood and followed. These policies cover the usage of all of the Information and Communication Technology (ICT) resources, including, but not limited to:

- All computer related hardware equipments, including desktop personal computers (PCs). portable PCs, terminals, workstations, wireless computing devices, telecom equipment, networks, databases, printers, servers, power supply equipment and shared computers and all network and hardware.
- All electronic communication equipments including telephone, radio communicators voice-mail, e-mail, fax machines, modems, PDAs, wired or wireless communication devices and services, internet and intranet and other on-line services.
- All software including purchased or licensed business applications, NIDC written

applications, employee or vendor/supplier written applications, computer operating systems and any other software residing on NIDC owned equipments, software bundled with any equipment

- All intellectual property and other data stored on NIDC's equipment.
- All of the above whether they are owned or leased by the NIDC or are under the NIDC's possession, custody, or control. All users, whether on NIDC property, connected from remote via any networked connection, or using NIDC equipment.

Definitions

The terms used have specific meanings in the context of this document and defined them here:

System:	Constitute hardware, software and communication devices
Hardware:	Also known simply as the computer or to the parts of the computer and its peripheral you can touch.
Software:	Also known as programs or sets of coded electronic instructions that tell the hardware what to do.
Data:	Refers to the raw facts that the computer can generate or process. It can consist of letters, numbers, sounds, or images.
File:	Is a set of data or program instructions that has been given a name.
Operating System:	It is the program that instructs the computer how to interact with the user and how to use devices such as the disk drives, keyboard, and monitor.
Connectivity:	It is the connection between workstation to the server. The connection between branches is also referred as connectivity. The connection is performed using guided (Lease line) and unguided (Radio Link, VSAT) medium.
Network:	Group of interconnected computers, servers and other peripherals devices.
IP Address:	The IP address refers to Internet Protocol (IP) address provided to all workstation, servers and network devices. This type of address resembles the address for all devices within a network.
WWW:	World Wide Web, prefix to denote website.
CPU:	The “central processing unit” is the computer’s processing hardware. It may consist of a single chip or several circuit boards.
Processor:	Is like the brain of the computer. It organizes and carries out instructions that come either from the user or the software.
Monitor:	Interactive display device, which displays input and output in the form of visual, characters and images.
The Management:	This implies to General Manager and Deputy General Manager(s) or designated person

2. Information & Communication Technology Infrastructure

2.1 Connectivity and Redundancy Connectivity

Connectivity of NIDC with its departments / branches will be made through Cable, Telephone lines, VSAT, Radio Modem, WIFI, Wireless, Communication Leased Line, Optic Fiber or any other connectivity medium. NIDC will maintain a primary connectivity along with secondary connectivity, which is required for redundancy purpose.

Viewing availability in the given location the choice of media should follow following precedence for quality, reliability, stability, scalability and transaction response time:

1. Fibre
2. Copper
3. Radio
4. Wifi
5. VSAT
6. Telephone (always as a last resort of backup)

In absence of dedicated point to point connection VPN should be used to secure all the communication from possible taping.

The backup lines should be maintained for branch connectivity, preferably through different service provider wherever applicable.

The secondary connection should preferably be from different service provider to minimize the down time.

The switching from primary to secondary and vice versa should be automated.

2.2 Network

Network Cabling

Network cabling is the interconnection of computers, inter & intra branches. The computers within a Branch are connected to each other by performing networking. The networking should be done within a Branch using category 6 (CAT 6) standard AT&T certified cables for its efficiency and performance. The network cable should be placed at least at a 9 inches distance from the power cables in order to avoid interference from power line.

At least a spare network cables need to be maintained for connections between main network switch and sub switch for fail over. The cable used for connecting branches through leased lines, radio link or other mode of communication should be regularly checked.

Always maintain spare networking equipments like switches, routers, patch panel, dial modem, lease line and radio modems (if in use). Redundant UPS supply (Primary and Secondary long hour Online UPS) with automatic fail over should be provided to all networking devices to avoid one point failure system which are most critical and sensitive.

All the networking devices should be of standard quality (preferably best in the market). The patch panel and switch used for networking should be placed within a metal rack inside the IT room in every branch. The rack should be used to keep modems, routers and other IT

equipments. Air conditioner should be installed in all System (Server) Rooms in all Branches.

The telephone cabling and network cabling should be done at every place where workstations and servers are in operation. The LAN and power cable diagram relevant to computer usage need to be maintained in every Branch. A set of copy should be maintained at IT Branch.

The faceplate, patch panel and switch should be labeled properly and should be of standard quality complying AT&T and CAT 6 Standards. The patch panel, routers, modems, switch and other networking devices should be kept in a secure location and only to be accessed by IT staff.

The printout of the configuration of routers, switches, firewall and modems need to be maintained and safely placed. A soft copy backup network device configuration should be taken on regular basis (monthly). The router setup password should be in dual custody of senior staff in IT Branch. Any changes in router setup should be logged and signed by both.

Access to Network

1. NIDC's entire network is to be closed user private network.
2. Every workstation with of PumoriPlus software at NIDC is a member of NIDC's domain.
3. Upon Management's approval a unique user name or user ID (Identification) and password are assigned to or created for staff in the network.
4. All users are required to log into the network using their own username and password.
5. The password should be at least 6 characters long (blank password are not permitted).
6. All users are required to change their password every 90 days and are notified by the system 5 days earlier from the date of expiry.
7. Users are not permitted to use the last 3 old passwords when changing his/her password.
8. Sharing of user name is strictly prohibited
9. Stealing of password and logging in using someone else's username is a serious offence and a staff so doing will be subjected to disciplinary action

NIDC's user is allowed to access NIDC's network through network connectivity. This part of policy is regarding usage and expected compliance related to network of NIDC.

Network Security

Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks. While IT Branch has responsibility for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating their own computer with ethical regard for others in the shared environment.

- Installation and configuration of firewall is to be done to ensure smooth functioning of network and to prevent from external threats.
- Physical security of the network equipments is to be installed, as required at the branches and Head Office as well.
- Configure the privilege to the access to the resources limiting the user only up to their needs as specified by the NIDC.

- User will be responsible for any security breaches or disruptions of network communication through their workstation. Security breaches include, but are not limited to, accessing data of which the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
- User will be responsible for interrupting any form of network monitoring which is not intended for the user, unless this activity is a part of the user's normal job/duty.
- User will be responsible for using any program / script / command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet / intranet / extranet
- Proper maintaining and monitoring of event logs on regular basis.

The following considerations and procedures must be emphasized in a network environment:

- IT Branch shall test all software before it is installed to make sure it doesn't contain a virus/worm that could have serious consequences for other personal computers and servers on networks.
- No other software shall be used other than those tested & approved by IT Branch.
- The choice of passwords must be made with great care to prevent unauthorized use of files on networks or other personal computers. Always backup your important files. Never store passwords or any other confidential data or information on your laptop or home PC or associated floppy disks or CD's or any other external storage devices.

2.3 Workstation

Installation

NIDC should maintain standard list of software for servers and the workstations. Each workstation is installed with this standard by the IT Branch. Access to such software installation files should be highly protected and to be used by the IT staff only.

IT Branch should periodically check all workstations meet this standard and verify the integrity of the products installed on them. Such standard list of software will be updated on time to time.

Upgrades

Workstations (hardware and software) must be upgraded regularly so that the products installed are compatible with the versions available at the time. During such upgrades, any security problems associated with the products must be identified and corrected.

Intervention

Whenever any sort of intervention is performed or needs to be performed on the workstation the User/Department Head/Branch Manager should contact IT Branch.

This part of policy is regarding usage and expected compliance in each workstation of NIDC.

- Each workstation will be defined as a member of respective domains.
- Workstation user identification will be created for each computer user.
- Network login for specified user will be restricted based upon official working hours or as may be advised by management from time to time.
- All workstations, PCs and laptops should be secured with a password protected

screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K / WinXP / WinVesta / Win7 users) when the host will be unattended.

- Every workstation must be shut-down properly before leaving the premises of NIDC.

Operating system's built-in policy management software tools should be implemented to prevent users bypassing the security rules and carrying out any unwanted modification.

2.4 Antivirus Guidelines

Latest anti-virus software from the leading anti virus software vendors should be installed on all workstations and servers. A parent server at the Head Office is where the latest virus definitions are to be downloaded on regular basis. Satellite servers should be set up in branches and/or where applicable in order to provide efficient protection to the local area network from virus threats. Virus definitions in satellite servers should be updated from parent server placed at the Head Office. All other workstations and servers should have Antivirus clients installed in them, which will retrieve latest virus definition file from their respective parent servers. An IT Supervisor monitors the working of the Antivirus regularly and generates reports at least on a quarterly basis. Head – IT Branch will review the reports and will recommend appropriate measures, if any, required to be taken, for the Management's approval.

The anti-virus program should be activated whenever a computer is switched ON so the user's actions may be monitored in real time. Users are prohibited to deactivate the anti-virus. Appropriate technical measures should be implemented to prevent users from disabling anti-virus program on their workstation.

This part of policy is to guide the users at NIDC control and protect them from any kind of risk of virus from any sources.

- Always run the corporate standard, supported anti-virus software available from the corporate download site. System Administrator will download, install and run the current version or anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, SUSPICIOUS or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your trash.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

3. Information & Communication Technology Ethics

3.1 User Profile Report

The end user ultimately has the responsibility for protecting the integrity of the equipment entrusted to him or her by NIDC. The users will abide by the rules in order to be able to use the computer and networking facilities (IT equipment) available to him/her. He or she is also responsible for protecting hardware, software & all the data contained therein, all of which are the NIDC's property. The end users are not authorized to remove or move any hardware from its original location.

This part of the policy is regarding user ID In Banking / Accounting software of NIDC.

- The software platform (ASP) user identifications (IDs) must be created / amended / deleted against approval of Management.
- User identification (ID) of staff on forced annual leave must be disabled for the period of such leave. IT Branch shall be intimated of such leave prior to such leave.
- All unused IDs / users must be deleted from the system. Such exercise must be carried out once in a month after review of all user list.
- There must not be any ambiguous / dummy IDs. In the event that such ID is required to perform a specific task, such ID may be created under the approval of system administrator and must be deleted immediately after completion of the specific task. Such use of authorized, deletion of dummy IDs must be recorded in writing in a register.

Use for Personal Business

NIDC's computing and network facilities may not be used in connection with personal work or for the benefit of organizations not related to NIDC. This and any other incidental use (such as electronic communications or storing data on single-user machines) must not interfere with other users' access to resources (computer cycles, network bandwidth, disk space, printers, etc.) and must not be excessive.

Use of Desktop Systems

Users are responsible for the security and integrity of the NIDC's information stored on their personal desktop system. This responsibility includes making, controlling physical and network access to the machine, and installing and using virus protection software. Users should avoid storing passwords or other information that can be used to gain access to other computing resources. Users should not store passwords or any other confidential data or information on their laptop or home PC or associated floppy disks or CD's or in any external storage devices.

3.2 Password

Password Construction and Management

Computer security is protected by passwords. A poorly chosen password may result in the risk of the NIDC's entire corporate network. As such, all account and network of NIDC's user will be protected by a password and the user is responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Password security isn't just a matter of thinking up a nice word and keeping it to you. User must choose a password, which will be difficult for someone else to guess or crack. We often have a tendency to forget passwords, so we choose something that has particular relevance to ourselves: the name of a loved one, our favourite car, sport, or ice cream, etc. Anyone knowing a little about us can make a list of these words and easily crack the password. All-digit passwords usually fall into this category - birth dates, phone numbers.

Observe the following guidelines when choosing your password:

- A password should be at least 6 characters long.
- Passwords must to be alpha numeric character with at least six figures / letters.
- Never make your password a name or something familiar, like your pet, your children, or partner. Favorite authors and foods are also guessable.
- Never, under any circumstances, should your password be the same as your username or your real name.
- Don’t use words that can be associated with you. Do not have a password consisting of a word from a dictionary. Most basic cracking programs contain words, and plenty of variations.
- Try to have a password with a number or mixed case letters. Simple substitutions like a '1' for an 'i', and '0' for an 'O' are easily guessed. Add a '%' or '$' to the middle of the password.
- Choose something you can remember, that can be typed quickly and accurately and includes characters other than lowercase letters.
- System-level password (e.g. root, enable, OS admin, application administration accounts, etc.) must be changed on quarterly basis.
- Protection system-level passwords must be part of the NIDC's administered global password management database.
- Back up of system level Administrators' password must be kept in hard copy in safe dual custody of authorized person as approved by GM / DGM.
- User-level password (e.g., email, web, desktop computer etc.) must be changed at least on every six months. However, the recommended change interval is on every four months.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- System should locked out Users (Intruder Lock) after 3 wrong login attempts. Only on written request IT Branch to unlock user.
- Any unusual and suspicious activities should be immediately reported to the IT Branch and the Management.
- Passwords should be memorized, never written down.
- Passwords belong to individuals and must never be shared with anyone else.
- New or changed passwords must be given in writing in sealed envelope only to the identified user whenever required, never over the telephone or via email.

3.3 Internet Usages

The new resources, new services, inter-connectivity available via the Internet, all introduce new opportunities and new risks. In response to the risks, this statement describes policy regarding Internet security. It applies to all staffs and members who use the Internet from NIDC.

The software for browsing the Internet should be configured in such a way that access to the Internet passes through the NIDC's security system called Proxy Server and Firewall. Latest Internet Exporer is the standard Internet browsing software. IT Branch shall frequently monitor user's activity and keep logs of the same. Any abnormalities should be reported to the Management for further action.

NIDC's computer network allows access to resources and services through internet connectivity. This part of the policy defines our policy regarding internet usages and expected compliance by users. This internet usage policy and its strict enforcement is an important and necessary part of the overall usage strategy. The internet usage policy applies to all internet users of NIDC who access the internet through the computing or networking resources.

The components in this document focus on issues associated with the NIDC's host computers, PCs, routers, terminal servers, and other devices that support access to the internet. The scope of this document does not include facility-specific usage policies, application usage, and· non-internet usage.

- Internet connectivity presents NIDC with new risk that must be addressed to safeguard the facility's vital information assets.
- Access to the internet by users who is inconsistent with business needs result in the misuse of resources. These activities may adversely affect productivity due to time spent using or surfing the internet. Additionally the company may face loss of reputation and possible legal action through other types of misuse.
- Access to the internet will be provided to user to support business activities and only on need basis to perform their jobs and professional roles related to NIDC with recommendation of Management.
- Internet access is to be used for business purpose only. Following standard internet services will be provided to user of NIDC as needed:
    1. Navigation - www services as necessary for business purposes, using a hypertext transfer protocol (http) browser tool.
    2. File Transfer Protocol (FTP) - send data/files and receive in-bound data/files, as necessary for business purposes.
    3. Send / receive Email messages to / from the internet (with or without document attachments).

The IT Branch shall, with the prior approval of Management, have the authority to block selected internet sites. The IT Branch can also direct users to specific site and block the rest depending on the needs and authority of the user.

3.4 Prohibited Usages of Internet

- Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.
- NIDC prohibits conduct of a business enterprise, political activity, engaging in any form of intelligence collection from facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.
- Using NIDC's computer resources to access the internet for personal purposes, without approval from the user's manager and the IT branch.
- Accessing NIDC's information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personal file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of company Web sites to other internet/ www sites whose content may be inconsistent with or in violation of the aims or policies or the company.
- Use, transmission, duplication or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Unauthorized downloading of any software programs or files for use without authorization in advance from the Information Technology Branch and the user's manager.
- Any ordering (shopping) of items or services on the internet.
- Playing of any games.
- Participation in any on-line contest or promotion.

Bandwidth both within NIDC and in connecting to the internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Users who choose to store or transmit personal information such as private keys, credit care numbers or certificates or make use of internet "wallets" do so at their own risk. NIDC is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

4. ICT Security

4.1 Physical Access

This part of policy is to establish the rules for the granting, controlling, monitoring and removal of physical access of information resource facilities. Technical support staff, security administrators, system administrators and others may have information resource physical facility access requirements as part of their function.

NIDC's physical access policy applies to all individuals within the NIDC that are responsible for the installation and support of information resources, individuals charged with information resources security data owners.

- All physical security systems must comply with all applicable regulations but not limited to building codes and fire prevention codes.
- Physical access to all information resources restricted facilities must be documented and managed.
- Access to information resources facilities must be granted only to NIDC's support personnel, whose job responsibilities require access to that facility.
- The process for granting code access to information resources facilities must include the approval of the person responsible for the facility.
- Each individual that is granted access rights to an information resource facility must receive appropriate training for the facility.
- Requests for access must come from the applicable NIDC's data system owner.
- Access codes must not be shared.
- Access codes that are no longer required must be returned to the person responsible for the information resources facility. Cards must not be reallocated to another individual by passing the return process.
- Lost or stolen access codes must be reported to the person responsible for the Information Resource facility.
- Codes must not have identifying information other than a return mail address.
- All information resources facilities that allow access to visitors will track visitor access with a sign in/out log book.
- A service charge may be accessed for access cards and/or keys that are lost, stolen or are not returned.
- Code access records and visitor logs for information resources facilities must be kept for routine review based upon the criticality of the information resources being protected.
- The person responsible for the information resources facility must remove the code access rights of individuals that change roles within the organization or are separated from their relationship with NIDC.
- The person responsible for the information resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

- The person responsible for the information resources facility must review code access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

4.2 Gateway to IT Branch

- System Administrators (SA) will be equipped with a specific code under the approval of Management for security of system. In order to maintain availability and security of SA code, System level code should be changed on quarterly basis.
- Gateway code has been provided for access to IT Branch. Authorized entrance to IT Branch must input the gateway code before the entrance. A separate log book is to be prepared for visitors to enter IT Branch. Visitors must be escorted in access controlled areas of IT by authorized person only.

4.3 Email

Preamble

e-Mail system in a work environment is an effective means of communication. However, it involves risks relating to theft of confidential material, the threat of virus and spy-ware infiltration. Therefore, giving email accounts to users should be monitored and documented and should be approved by the Management. Electronic mail and communication facilities are intended for official purposes. This part of the policy covers appropriate use of email sent from the NIDC's email address and applies to all users operating on behalf of NIDC. To protect public image of NIDC through all outgoing email, an official message,

> *"© Nepal Industrial Development Corporation, NIDC. All rights reserved. This message is for information purpose only and its content should not be constructed as an offer, or solicitation of an offer, to buy or sell any banking or financial instruments or services and no representation or warranty is given in respect of its accuracy, completeness or fairness. You should take your own independent tax, legal and other professional advice in the respect of the content of this message. This message may not be copied, redistributed or published (in whole or in part) without our prior written consent. This mail may have been intercepted, partially destroyed, arrive late, incomplete or contain viruses and no liability is accepted as a result. The information in this email is confidential and is intended solely for the addressee(s). Access to this email by anyone else is unauthorized. If you are not an intended recipient, you must not read, use or disseminate the Information contained in the email and notify the sender, except where the sender specifically states them to be in views of NIDC".*

will be sent from NIDC on each and every email.

- NIDC's email system shall not be used for creation or distribution of any distribution or offensive messages, including offensive comments about race, gender, hair color, disabilities, age sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Users who receive any emails with this content from any second party should report the matter to their supervisor immediately
- Using a reasonable amount of NIDC resources for personal emails is acceptable, but non work related email shall be saved in a separate folder from work related email.
- Sending chin letters or joke emails from NIDC's email account is prohibited.
- NIDC's employees shall have no expectation on privacy in anything they store, send or receive on the NIDC' email system. The NIDC's IT Branch may monitor messages without prior notice.

- NIDC's email system shall not be used for sending unsolicited email messages, including the sending of "junk mail" or other advertising material to users who did not specifically request such material (email spam).
- NIDC's email system shall not be used for any form of harassment.
- NIDC's email system shall not be used for unauthorized email originating from within NIDC networks of other internet/intranet/extranet service providers on behalf of, or to advertise any service hosted by NIDC or connected via NIDC's network.
- Users are bound by ethical standards when using the official email account. One shall not forward chain mail, jokes, personal photos, and obscene materials.

4.4 Scope

The terms and conditions under which the Bank staff can avail e-mail facility are broadly mentioned below.

4.5 Policy Definitions

Account: The credentials issued to a user for authentication and access control to an email system, generally consists of a User ID and password, which is granted upon the Management's approval.

Address: E-mail address (generally in the form user_first_name@domain), which identifies the sender or recipient of e-mail message.

Mailbox: Storage location on an e-mail system where messages are received and stored.

Message: An electronic record (including attachments), created, sent or received amongst email users on an e-mail system.

4.6 Policy Provisions

NIDC is the owner of all e-mail accounts and e-mail addresses in its registered domains. All e-mail messages processed by NIDC e-mail server become the property of NIDC.

- The Management reserves the right, without notice, to inspect, modify, return, reject, redirect or discard any e-mail message it receives.
- Staffs are assigned minimum mailbox of 50MB in storage size for their email account that includes space occupied by the hidden system files and folders.
- Management reserves the right to terminate any e-mail account without prior notice.
- Identification and authentication is exclusive to each e-mail user and may not be divulged. Each account is personal and cannot be used by a third party.
- Users should not unnecessarily or frivolously overload the email system. Spam and junk mail, chain mails and attachment files that are not job related is prohibited.
- The end user must not modify the e-mail software components and email parameters locally. The user may not use means, other than the NIDC email system on his workstation to send/receive email messages. Systematic redirecting of email to an off-premises email address is forbidden, for reasons of confidentiality.
- Email users should not send emails with attachments with such extensions as exe, com, scr, gif, jpeg, dat and zip.
- Unauthorized entry into other's email account is strictly prohibited. Only the IT Branch, with the written approval of the Management, shall have the authority to enter other staff's email account. Such approval will be given in writing and on a need basis.

- Email should not be used for the purposes that are in conflict with NIDC's interests. Email users must not use the email system to send, even to trusted correspondents, any sensitive information (user IDs or access codes or other in-house information), data covered by organization's secrecy (financial status etc.) or, in general any data whose disclosure or alteration during transfer could be damaging to NIDC, without first taking adequate security precautions (encryption, digital signature). End users must be regularly informed in this regard.
- Users should practice to activate Out-Of-Office message service while in long holidays (more than 3 days).
- Email containing a formal authorization, approval, or handling of responsibility must be printed on paper and filed appropriately for purpose of evidence and accountability as it may be required at a future date.
- Mail filtering application shall be implemented on the email server by the IT Branch to filter out all unnecessary and potentially harmful attachments from emails right at the email server.
- A disclaimer will be attached to every out going messages. Users are not permitted to change or remove this disclaimer and users should abide by the content of disclaimer.

4.7 Data Security

This part of the policy is to establish for the security of database configuration of internal server equipment that is owned and/or operated by NIDC.

The objective of the policy is to ensure that due care is exercised in protecting NIDC's computing systems and data.

- Access to IT Branch will be limited to IT staff, Operation Managers, Branch Chiefs, Auditors and Management. Any unauthorized entry shall be strictly prohibited. Similarly gateway to the IT Branch must be code protected. This is to be provided to authorize person only. IT Branch must be locked at all the time. A visitor's log book must be maintained in the unit to record entry or visitors other than the authorized persons. Any unauthorized entry should be escorted by authorized person and entered in a visitor's log book.
- IT Branch will maintain hardware/software error/problem log book and any error/problem sighted/identified must be recorded with details such as reason or error/problem and action taken to sort out the problems. All error/problems must be reported to the IT Branch Chief and record of this action must be logged in the logbook maintained in IT Branch. This logbook shall be reviewed by Branch Managers in case of braches and by Management in case of Head Office on a monthly basis.
- One set of Offsite Backup tapes are to be under the custody of the person/staff as delegated by Management and other set is to be stored in vault everyday. These custodian(s) are responsible for the safe keeping of the tapes at their residence. An alternate custodian must also be nominated by Management and the alternative custodians will be responsible for the custody of these back up tapes in case of emergency and/or the first custodian is on leave or absent for any reason. If the first custodian is to go on leave, he/she must handover the tapes to the back up custodian before proceeding for leave. Further the alternate custodian will be responsible to retrieve the tapes from the first custodian in case of the emergency.
- Each user will be provided individual user IDs and password for network access, email, PumoriPlus etc. any of the passwords belonging to a user must not be shared with others. The users must log out from the system when they are not using the system so

that no other can misuse his/her password. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K / WinXP / WinVesta / Win7 users) when the host will be unattended.

- Each user / employee will be responsible for proper use of NIDC's IT system.

4.8 Power Equipment/Accessories

Every computer (workstation) must be connected through Uninterruptible Power System (UPS). Each UPS must be connected through power conditioner of similar capacity. The main servers should be connected through redundant on-line UPS with minimum power backup of 4 hours and with auto fail over system. The UPS, both online and offline should be of good brand and quality. Any disruption in power will bring down entire system to halt. There should be at least one generator with auto start facility. Viewing in excess of 20 hours load shedding as experienced in earlier years it is suggested to have smaller generator just to cater load at IT Branch facility and Cold Room (room housed for servers and other critical networking equipments.

4.9 Hardware Standards

Every hardware should be of good brand and of good quality. It is recommended to shortlist three top brands on each category while purchasing any hardware. This way, the total cost of ownership will be much less with minimal downtime. The operating and maintenance cost will also be minimum. Any hardware should be purchased only if the local support and required resources is available locally. There should be some standard products through out the organization to bring down support cost and spare part cost. The heterogeneous environment always brings chaotic situation increase downtime and increasing support cost. Every hardware including power supply system should be under Annual Maintenance Contract maintaining requisite spare parts either by organization or by support vendor. All the hardware equipment should be provisioned to be replaced in every five years. This will help to keep abreast for any changes in future. Otherwise, outdated system might bring more costly solution while updating or enhancing the system

4.10 Software Standard

All software should be legal copy. The organization should not be using any pirated software. As in the case of hardware all software should be of good brand and good quality with proper local support. There should be Annual Support for all the software purchased. The software should be updated only timely manner rather than waiting for last hour. The top three software should be listed while evaluation.

4.11 USB Drives

USB port of all the computers should be disabled from the day first. The activation of USB port in any required computer should be done only upon Management’s approval.

4.12 Magnetic Tape Drive

The data of mission critical system should be backed up on regular basis in Magnetic Tape. Procedure to be followed:

1. Daily backup (Sunday to Saturday and rotate)
2. Weekly back (A, B, C and rotate)
3. Monthly backup (have separate tape for each month and store it for future referral).

Two sets of backup should be taken. One set to be stored at production site and another set should be stored off-site location with locker facility with easy access (24*7).

A set of tape drive should be kept separately for emergency use or in future use with relevant drivers.

4.13 DVD/CD ROM Drives

All DVD/CD ROM drive should be disabled before deploying workstation for staff use. The activation of such drive should be done only upon Management's approval

4.14 Data Storage Policy

Once the data is loaded to a longer-term file space (floppy disk, tape cartridge, CD, etc.) it must be protected against unauthorized access. Data should not be located in area accessible via the network by unauthorized persons.

IT Branch should develop a robust network and data storage infrastructure that enables staff to store and access critical and official data from multiple locations in secured and protected network directories. It is not intended to archive large amounts of non-critical or personal data.

The files or documents, which do not carry the Banks ownership, are prohibited from being stored in computers, which are the NIDC's resources.

Given the exponential growth of business volumes coupled with a limited storage capacity of the server there is a need to restrict storage of data in the on line server.

Accordingly, as a policy, the storage of data in the on line server shall be restricted to two years, including the current year (1+1 years).

Data, older than two years, is to be archived in a non–online server. However, in case of need, arrangement shall be made for selected users to access the non–online archived materials/data.

4.15 Cold Room for Servers

Servers hold very important and sensitive information/data of the organization and hence, maximum precaution should be taken in preserving the integrity of the servers and the database it holds, this includes critical networking and communication equipment. Due to the nature of the server and high frequency of its usage, its electrical devices and circuits are vulnerable to burnouts and malfunction as a result of excessive heat. Therefore, these equipments are to be isolated and kept in a cool/air-conditioned environment. The temperature in this cool environment should range from 16 to 21 degree Celsius. It is preferable to have redundant air conditioner for fail over.

Periodic maintenance of the air conditioner should be carried out to ensure that they are working at an optimum and with no water leakage. De-humidifier should be installed.

Proper fire extinguisher should be installed within the proximity of easy access.

4.16 Power Cabling

Power is the essential element for all components–electrical, electronic-to work. Power needs to be maintained and cabled properly in order to avoid power disasters. For power management the following matters need to be taken into consideration:

The three-phase line (single phase line in rural areas, depending upon load) should be inducted. All the phases should have balanced load and be checked for leakage. There should be an agreement for support on electrical works. Proper, separate earthings should be placed for normal electrical appliances, computer equipment, ATM, Generators, Air Conditioners (A/Cs), etc. from the day first.

Generator with auto-start feature should be provided as a backup power supply incase of main line failure. There should be an agreement for regular maintenance of generator.

To protect equipment from city line's high voltage surge and spike, High Voltage Protection devices shall be installed in all Line Distribution Boards (viz. city lines, Uninterrupted Power Supply (UPS) lines, generator supply lines).

Each computer installed site should have an UPS of sufficient load (using maximum 70% of UPS capacity) for supplying power to all IT related equipment. The power supply to UPS should be through power conditioners. The power conditioner is used to filter the city line for surge, spike and noise. This ensures clean and consistent power is supplied to electronic devices.

The main line and UPS line should be provided to all the places where workstations, servers and IT equipments are in operation. These lines are differentiated using a round socket for the main line and flat socket for the UPS line. The socket should be of good quality and quality standard need to be maintained.

The vendor under the contract/agreement should maintain monthly log of power load, power leakage, condition of earthings and cables, etc. Given the sensitive nature of the equipment monthly maintenance of electrical supplies and generator should to be carried out.

IT Branch should maintain a list of electrician contacts and hot line number(s) of the Electricity Authority. Standby electricians should cover maximum business hours in case of power failure.

4.17 Physical Protection

Workstations and servers are property of the NIDC, any change or modification (even changing of location) of such is to be notified and approved by the IT Branch beforehand. In accordance with the Bank's policy only the IT Branch, after approval of Management, has the authority to make any physical modification to the workstation and its components. An updated inventory of workstations, printers, scanners and other accessories shall be maintained by the IT Branch with a copy to Account Department.

All the workstations and the servers must be physically protected. Specially servers, storage media (tape drives), heavy duty printers must be kept in separate system room (as part of physical protection) accessible only to authorized persons (viz. IT staff and the Management).

5. ICT Disaster Recovery Plan

5.1 Introduction

This Information Technology (IT) Disaster Recovery Policy (DRP) presents the requirements, and the steps that will be taken in the event of any disaster affecting IT services at NIDC, with the fundamental goal of allowing basic business functions to resume and continue until such time as all systems can be restored to pre-disaster functionality.

Response to and recovery from a disaster at NIDC is managed by the Central Support Group (CSG).

The Bank should established a Disaster Recovery Site (DRS) preferably at different seismic zone with availability of all pre-requisite facilities such as communication link, stable city power supply, easily accessible road, good concrete building with earth quake resistible. This site should be taken as “Cold Recovery Site” for quick recovery of the data. The site should contain online replication of main centralized server hosting database along with all other equipment including printers and papers.

Scope

Due to the uncertainty regarding the magnitude of any potential disaster, this plan will only address the recovery of systems under the direct control of the IT Branch, and that are considered critical for business continuity to discharge basic business functions. The following major areas are addressed in this plan in the given precedence:

- Mission critical software system
- Data Network and Data communications

This plan covers all phases including:

- Incident Response
- Assessment and Disaster Declaration
- Incident Planning and Recovery
- Post Incident Review

Assumptions

The Disaster Recovery Policy is based on the following assumptions:

1) Once an incident is declared a disaster by the Central Support Group it will take over the responsibility and the appropriate priority will be given to the recovery effort with available resources and supports.
2) The staff and employees are of prime importance and the safeguard of such will supersede concerns specific to hardware, software, and other recovery needs.
3) Depending on the severity of the disaster, other departments/divisions may be required to modify their operations to accommodate any changes in system performance, computer availability and physical location until a full recovery has been completed. The IT Branch will encourage all other departments to have Business Continuity Plans for their operations, which include operating without IT systems for an extended period of time.
4) The content of this plan may be modified and substantial deviation may be required in the event of unusual or unforeseen circumstances. These circumstances are to be

determined by the specific Disaster Recovery Teams, under the guidance and approval of the Central Support Group (CSG).

5.2 Disaster Preparedness

A critical requirement for disaster recovery is ensuring that all necessary information is available to assure that hardware, software, and data can be returned to a state as close to "pre-disaster" as possible. Specifically, this section addresses the backup and storage policies as well as documentation related to hardware configurations, applications, operating systems, support packages, and operating procedures.

Vital Computer Stationary Stocks: Administration Department (GSD) shall maintain a one week stock of items used by IT Branch at off-site.

Data Recovery Information: Backup/recovery tapes are required to return systems to a state where they contain the information and data that was resident on the system shortly prior to the disaster. A set of backup tapes is stored in an on-site and another set at off-site locations (at DR site).

Server Recovery Information: In the event of any disaster, which disrupts the operations in the IT Branch or EDP/System room at the respective Branch, reestablishing the data will be the highest priority and a prerequisite for any IT recovery. As such, IT shall have detailed information and records on the configuration of all the servers and ancillary equipment located in the IT Branch and, in the DR site.

Network & Data Communication Recovery Information: In the event of any disaster which disrupts network and/or data communication operations, reestablishing connectivity will be a high priority and a prerequisite for IT recovery. As such, IT is required to have detailed information and records on the configuration of all networking equipment.

Desktop Equipment Recovery Information: Information necessary for the recovery and proper configuration of essential desktop computers and printers to cater basic business functions is critical to restore to a configuration equivalent to pre-disaster status.

5.3 Disaster Recovery Processes and Procedures

In the event of an incident affecting any portion of IT infrastructure, several key steps must be taken to assure that the level of response is appropriate, well coordinated, and assures that the highest priority of safeguarding personnel is achieved. The following section of the policy outlines these steps, and the decisions to be made throughout the process.

Emergency Response: Emergency Response Team's (ERT) involvement and the membership of the ERT will be dependent on the size and type of the incident. In addition, the actions of the ERT will be accomplished prior to the execution of this plan. Examples of situations, which will normally result in the involvement of the ERT, include:

- Severe structural damage to the facility where personal safety is in question, and where analysis must be completed to assure the building is acceptable for access. This would include, but is not limited to, damage from an earthquake or tornado.

- Environmentally hazardous situations such as fires, explosions, or possible chemical or biological contaminations where the situation must be contained prior to building occupancy.
- Flooding or other situations, which may pose the risk of electrical shock or other life-threatening situations.
- Major system/hardware failures that do not pose a hazard to personnel or property.
- Utility outages (electrical, etc.), which are remote to the IT facility being affected.

Incident Occurrence: Upon the occurrence of an incident affecting the IT services, Head of IT Branch and Administration Department will be notified by Bank's security and/or other personnel. Personnel reporting the incident will provide a high-level assessment as to the size and extent of the damage. Based on this information, the IT Branch Head will assume responsibilities as the Incident Manager (IM), and will contact the other team members and determine the following:

- Brief overview of the incident, buildings affected, etc.
- Which Incident Command Center (ICC) will be used.
- Scheduled time to meet at the ICC for initial briefing.
- Any additional information beneficial at this point. No other staff members are to be contacted at this point, unless directed by the Incident Manager. Incident Command Center (ICC) locations are:

  Primary:

  Secondary:

  Backup:

Should all of these facilities be rendered unusable, it is assumed that the disaster was "catastrophic" in nature and that the technology recovery effort will be secondary to other concerns. At this point, the IT Incident Manager will work closely with overall Central Support Group (CSG) to determine the appropriate course of action. The Incident Manager is responsible for locating an alternate site for the team and revaluating the best strategy for recovery.

Incident Assessment: The Central Support Group will receive an initial briefing from the Incident Manager (IM) and any other personnel invited to the meeting. The CSG will assess the situation, perform a walk-through of affected areas as allowed, and make a joint determination as to the extent of the damage and required recovery effort. Based on this assessment, the team will make a determination as to whether the situation can be classified as "routine" and handled expeditiously via normal processes, or if a formal IT disaster needs to be declared.

- Routine: Area(s) affected by the incident are identified and the appropriate personnel are contacted to report to work to evaluate and resolve the situation.
- Disaster: The Incident Manager contacts the Central Support Group (CSG), notifies him/her of the situation, and that an IT Disaster has been declared. The CSG identifies which areas of the IT infrastructures are affected, and contacts the members of the specific Disaster Recovery Teams. Team members are provided with the following information:
  - Brief overview of what occurred

- Location and time for teams to meet
- Additional information as required.

Once an IT disaster has been declared, and the preceding steps to notify the Management Team and the Recovery Teams have been accomplished, ongoing responsibilities of the Central Support Group and Incident Manager include:

- Securing all IT facilities involved in the incident to prevent personnel injury and minimize additional hardware/software damage.
- Supervise, coordinate, communicate, and prioritize all recovery activities with all other internal / external agencies. Oversee the consolidated IT Disaster Recovery plan and monitor execution.
- Hold Disaster Recovery Team meetings/briefings with team heads and designees as and when required.
- Appointing and replacing members of the individual recovery teams who are absent, disabled, ill or otherwise unable to participate in the process.
- Provide regular updates to the Management on the status of the recovery effort. Only the Management and/or their designees will provide updates to other agencies (media, etc.)
- Approve and acquire recovery resources identified by individual recovery teams.
- Interface, coordinate and interact with other activities and authorities directly involved in the Disaster Recovery (Police, Fire, Department of Public Works, etc.).
- Identify and acquire additional resources necessary to support the overall Disaster Recovery effort. These can include acquiring backup generators and utilities, arranging for food/refreshments for recovery teams, etc.
- Make final determination and assessment as to recovery status, and determine when IT services can resume at a sufficient level to discharge basic business functions.

5.4 Disaster Recovery Teams

Disaster Recovery Teams are organized to respond to disasters of various type, size, and location. Any or all of these teams may be mobilized depending on the parameters of the disaster. It is the responsibility of the CSG to determine which Disaster Recover Teams to mobilize, following the declaration of a disaster and notification of the Management.

Each team will utilize their respective procedures, disaster recovery information, technical expertise, and recovery tools to expeditiously and accurately return their systems to operational status. While recovery by multiple teams may be able to occur in parallel, the IT Branch and Network/Data Communications infrastructure will normally be assigned the highest priority, as full operational recovery of most other systems cannot occur until these areas are operational.

Network & Data Communications Recovery Team

- Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
- Assess damage and make recommendations for recovery.
- Identify other individuals required to assist in recovery of network services, and report this information to the IM for action.

- Develop overall recovery plan and schedule, focusing on highest priority areas of the Bank infrastructure first.
- Coordinate hardware and software replacement with vendors.
- Oversee recovery of data communications and the network services based on established priorities.
- Coordinate network and data communications recovery with other recovery efforts
- Provide scheduled recovery status updates to the Incident Manager (IM) to ensure full understanding of the situation and the recovery effort.
- Verify and certify restoration of the Network & Data communications infrastructure to pre-disaster functionality.

Data Center Recovery Team

- Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
- Assess damage and make recommendations for recovery.
- Identify other individuals required to assist in recovery of the data application, and report this information to the IM for action.
- Restore degraded system function at backup site and inform end users on restrictions on usage and/or availability of system facilities.
- Coordinate software replacement with vendor as required.
- Coordinating data system recovery with other recovery efforts.
- Execute plan to restore of data to full function.
- Provide scheduled recovery status updates to the Incident Manager (IM) to ensure full understanding of the situation and the recovery effort.
- Verify and certify restoration of the application data to pre-disaster functionality.

Desktop Recovery Team

- Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
- Assess damage at all areas affected, and make recommendations for recovery.
- Identify other individuals required to assist in recovery of desktop services, and report this information to the IM for action.
- Develop overall recovery plan and schedule, focusing on highest priority areas of the organization infrastructure/desktop services first to discharge basic business functions.
- Coordinate hardware and software replacement with vendors.
- Oversee recovery of desktop computing services (workstations, printers, etc.) based on established priorities.
- Coordinate recovery with other recovery efforts.
- Provide scheduled recovery status updates to the Incident Manager to ensure full understanding of the situation and the recovery effort.
- Verify and certify restoration of the desktops to pre-disaster functionality.

5.5 Possible Risks, its Prevention and Recovery Plan

Possible areas that could affect customer service and/or internal daily routine task:

Mission Critical Application Server

Access to this server is restricted to all users during regular time except the Administrator user. Only incase of disaster access to server will be permitted by the Administrator.

Mission Critical Application Data

Data Backup

Generator

Every office should have one generator for it's emergency use in addition to UPS. The transaction could be continued for 5-10 minutes depending upon the load on UPS even if both city line and generator is failed.

Miscellaneous

All original and copy of agreements related to IT Branch should be kept safely inside a fire resistant vault within IT Branch. (Appendix A).

All original diskettes and CDs of critical software used in the Bank should be kept safely inside fire resistant vault within IT Branch. (Appendix B).

All software manuals (Appendix D) and internal approved memos (old ones) should be kept safely in fire resistant vault within IT Branch.

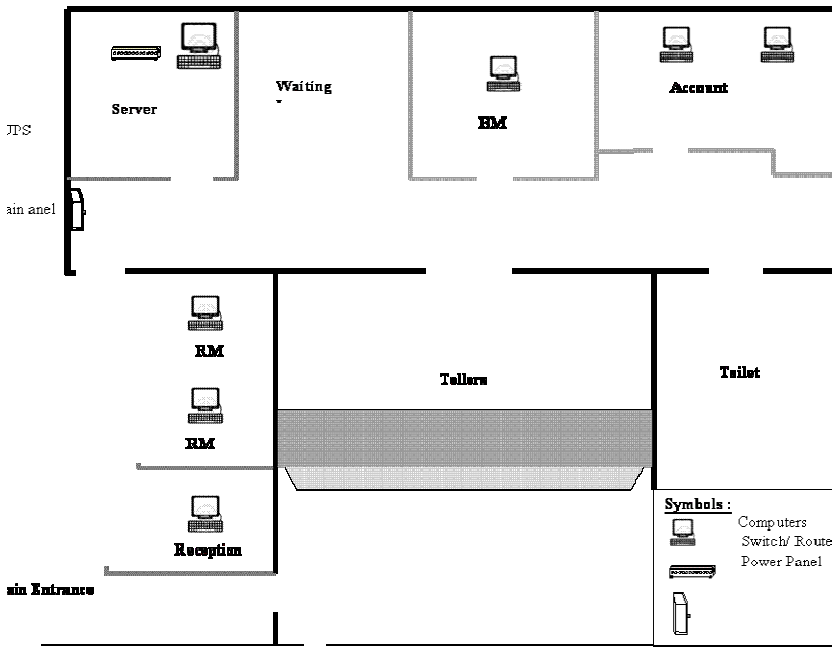
All keys (Appendix C) and documentations related to IT Branch should be kept safely in fire resistant vault within IT Branch.

A copy of daily, monthly, yearly data backup tape cartridges of all the databases present in Head Office server should be stored safely in fire resistant vault within IT Branch.

Grab List

The staff of IT Branch should grab the items/documents (if possible) listed in Appendix F on the way out if an incident occurs during office hours.

IT Branch Layout with Equipment Location



5.6 Disaster Recovery

In order to ensure smooth and timely recovery of data / information, the following procedures are to be followed by IT Branch:

Primary / Secondary Servers

IT Branch shall be equipped with two servers (Primary and Secondary). Daily operations are carried / processed by the Primary Server and the Secondary Server is kept at stand-by backup. It shall be ensured that the Secondary Server can be upgraded to Primary Server in a short period of time, if required.

Onsite / Offsite backup

The NIDC System data files are to be backed up and kept on-site as well as off-site for security purposes. The data back-up files generated by banking / accounting software as and when installed before and after the end of day processing are copied in the Secondary Server on a daily basis as on-site backup.

- After of end of day, these files must be fully backed up in a magnetic tape by the System Administrator and must be taken home daily by authorized person as designated by G.M.
- In order to test the functionality and the accuracy of the information contained in the tape, it is required to test the backup tapes regularly on a quarterly basis by System Administrator.

6. ICT Policy Review and Monitoring

6.1 ICT Steering Committee (ICT-SC)

The ICT - Steering Committee (ICT-SC) is formed by GM Monthly meeting is to be held to discuss issues related to IT. IT Branch will handle IT relates issues under the guidance of this committee. ICT Steering Committee or its designate may authorize changes / amendments to procedures specified herein, as may be required from time to time.

Table 1: Members of ICT-SC

S. No.	Position in NIDC	ICT-SC Position
I.	General Manager	Chairperson
2.	Deputy General Manager (Operations)	Member
3.	Head, Commercial Banking Division	Member
4.	Head, Accounts Division	Member
5.	Head, IT Branch	Member Secretary

After every meeting a minute of the meeting will be drafted by Member Secretary and to be signed by chairperson and all members of the committee.

Appendix A - List of critical documents stored in fire resistant vault

It shall enlist all the important documents (IT related or otherwise) kept in the vault for safe keeping. eg. Original license document of banking system etc.

Appendix B - List of Original CDs/diskettes in fire resistant vault

It shall enlist the title and number of CDs/DVDs related to software installed in the NIDC computers, including banking computers. For example, software CD/DVD of PumoriPlus, Antivirus, Windows Server etc.

Appendix C - List of IT Branch held critical documents stored in fire resistant vault

This list includes all the agreement documents, memos of management approved relating to Information and Communication Technologies (ICT), e.g. Original license agreement of PumoriPlus, Annual Maintenance Contracts (AMCs) with various vendors, Authorization approvals etc.

Appendix D - List of software manuals kept in fire resistant vault

This includes number and details of manuals related to software installed in NIDC computers, including commercial banking and elsewhere. The typical documents includes PumoriPlus banking software manuals; Windows Server installation and operating manuals etc.

Appendix E - Team Members and Contact Information

Central Support Group (CSG), a specialized group dealing with Data Management and IT solutions, shall be formed and comprise of IT Branch Head, System Administrator, Mercantile personnel, Deputy Director of General Services Branch and any other IT related staffs (in-house or on-call) sought by NIDC Management. CSG shall be responsible for smoothly running the Banking operations. CSG shall specify persons to deal with Incident Management, Desktop Recovery, Data Center Recovery, Network & Data Communication Recovery etc.

A list of CSG members with following corresponding information shall be prepared for use in emergency.

CSG Coordinator: Head IT Branch

Name	Position	Address	Telephone & Cell No.

Name of person responsible for Incident Management (IM):

Name of person responsible for Desktop Recovery (DTR):

Name of person responsible for Data Center Recovery (DCR):

Name of person responsible for Network and Data Communication Recovery (NDCR):

This list shall be reviewed at least once a year and updated as and when required.

Appendix F - Grab List

- Routers
- Modems (both lease line and radio)
- Tape Drive
- Tape Cartridge of all applicable backups (PumoriPlus Database backup, email server backup, fileserver backup etc.)
- CPU of the server
- Keys of vault
- Backup and Restore Procedure
- Disaster Recovery Procedure
- Hardware Inventory List
- Router Configuration list
- UPS and power conditioner

Appendix G - Equipment in Cold Room

This includes equipments placed in cold rooms, eg. Servers, Routers etc.

Safe keeping of all original software CD and documents inside Fire Resistant Vault
Contents:

Appendix H - Vendor Contact List

All the contact information of Hardware, Software, Peripherals and all other ICT software and hardware vendors to be enlisted.

Appendix I - Vital Computer Stationary Stocks

The list will vary as per consumption, so it shall be updated accordingly, so as to keep track with the remaining stocks sufficient for smooth operation of NIDC activities.