Policy #1 - Justifying and Acquiring Computers

It is the policy of xxxxxxxxxxx to use computers in applications where material benefits can be realized in improved customer service, increased productivity, better access to information, and/or lower overhead cost of delivering products and services.

The purchase of each individual computer and related software must be justified on the basis of the above criteria.

Procedure #1 - Justifying and Acquiring Computers

Justification

Computers at xxxxxxxxxxx are usually depreciated over a three year period. If a computer is less than three years old and a replacement is requested, the Department Manager must submit a *written proposal* to the Information Systems Department explaining why the computer needs to be replaced. This written proposal will accompany a Fixed Asset Form which requires Division Head approval.

Computers more than three years old may be replaced upon request of the Department Manager or recommendation of the Information Systems Department. A Fixed Asset Form, requiring Division Head approval, must be completed.

Major purchases are those where the cost is greater than $10,000. Typically, these purchases will consist of the purchase of hardware and a third-party software application *specific to a particular business unit.* This type of purchase must be justified - *in writing* - by the Department Manager through an evaluation of cost versus expected benefits (i.e., better customer service, improved efficiency, improved productivity, quality, etc.) This written proposal and a Fixed Asset Form must be completed and will require signatures from the Division Head and the Chairman/President. Purchases greater than $25,000 also require Board approval.

Fixed Asset Approval Limits are as follows:

Division Head - up to $10,000.
Division Head and President/CEO - up to $25,000
Division Head, President/CEO & Board of Directors - over $25,000

Acquisition

The Information Systems Department will coordinate the delivery by the vendor of the acquired equipment to the Information Systems Department or User Department.

The Information Systems Department will review the delivered equipment and/or software to ensure that it is complete and in condition for the User Department to utilize.

The Information Systems Department will include this newly acquired hardware and/or software on the appropriate inventory records.

The Information Systems Department will coordinate the installation and configuration of equipment as well as the installation and configuration of software products.

When necessary, the User Department will submit a request for training to the Information Systems Department.

For major system purchases consisting of a third-party application specific to that department, the User Department Manager may request software training directly from the vendor.

Policy #2 - Implementation of Software

It is the policy of Xxxxxxxxxxx that no applications will be developed in-house utilizing program languages unless written authority is given to do so by the Information Systems Department.

All users are equipped with a computer and access to software that is contained on the Recommended Software List (see Appendix.)

In most cases, software purchased by the Information Systems Department for use on computers will include a Software License Agreement. These software licensing agreements (i.e., single-user license, site license and/or multiuser license) protect proprietary software packages per federal copyright laws. It is the policy of Xxxxxxxxxxx to adhere to these licensing agreements.

Procedure #2 - Implementation of Software

Specialized software packages must :

1. Satisfy the perceived need of the user.
2. Be properly documented in accordance with established standards.
3. Provide for proper controls, file backup; and retention.
4. Utilize a Abusiness expert@ from the User Department to work with the Information Systems Department.

Any software to be developed and/or acquired which would produce results which would affect financial reporting or Generally Accepted Accounting Principles must be approved by the Chief Financial Officer.

User Departments should properly test all specialized software applications prior to implementation to ensure that the software works as desired and that the results obtained are accurate.

Policy #3 - Copyright Protection

The Software and Information Industry Association enforces copyright protection laws. Significant fines are assessed to individuals/entities that utilize illegal copies of software. Illegal copies of software are those *where licensing agreements do not accompany the software installation.* It is against bank policy to utilize software that does not have an associated licensing agreement (i.e., pirated software) on any of the bank=s computers.

Procedure #3 - Copyright Protection

When purchasing software, Xxxxxxxxxxx will utilize the appropriate licensing agreement as defined by the vendor (i.e., single-user version, concurrent license, site license, network version, etc.) Software is centrally located within the Information Systems Department along with the associated licensing agreements.

Users are not allowed to install software on a bank computer. Nor are users allowed to copy (*or otherwise attain*) bank-owned software and install it on a computer outside the bank.

Because the bank is ultimately responsible and accountable for its employees= compliance with the software copyright law, software installations are subject to audit by the Information Systems Department and/or the bank=s internal auditing staff. The audit can be performed on the user=s *local hard drive* and the bank=s fileservers.

Policy #4 - Physical Security for Corporate Information

The vast majority of corporate information is stored on the bank=s fileservers. Corporate fileservers, wherever possible, are in physically secured areas.

Corporate fileservers and LAN/WAN communications equipment resident at the corporate headquarters are physically secured within the computer room. The main power supply enters the facility from two different power feeds. A dedicated air conditioning unit is located within the secured computer room. In addition, Xxxxxxxxxxx has an un-interruptible power supply (UPS) located in the same secured room. An emergency generator (diesel powered) is prepared to activate immediately if both power feeds are disrupted to provide electric power to certain, pre-established locations throughout the building complex. The entire computer room and telephone communications rooms are connected to emergency power.

Data communications also has redundancy at the corporate headquarters. A SONET Ring enters the building from two different locations and feeds back to the Verizon Central Office located in downtown New Bedford. This provides automatic re-routing of all data and voice traffic should one of the circuits be severed. In addition, there are analog copper circuits and ISDN circuits to provide additional protection.

In the event of some disaster in the computer room, the bank has identified the second floor of its Plymouth Central Office to be designated as a Acold site@ where emergency operations would be established. Please see the Business Resumption Plan for more details.

The computer room is restricted to only those employees authorized to enter the restricted area. Further, an intrusion security alarm must be activated in the evening and de-activated in the morning before entering. All access is monitored with a Security Control Access Card System. Only a limited number of authorized employees are allowed entry in to the computer room. Visitors must be accompanied while in the computer room. Video cameras at the corporate headquarters are used to monitor main building entrances, as well as the loading dock and shipping/receiving areas and all elevator lobbies. Xxxxxxxxxxx uses a security Aproxy@ card to control access to the building and each floor. In addition, different control levels are required to access the computer and telephone communication rooms. A security administrator in Corporate Services tracks and cancels the Aproxy@ cards as changes occur. Card reader usage is automatically logged by the card key system.

Some information, specific to a particular user, is stored on the user=s computer (i.e., workstation and/or notebook PC.) It is the user=s responsibility to maintain the integrity of information stored on these computers and to prevent unauthorized access.

Procedure #4 - Physical Security for Corporate Information

The following steps should be taken for the physical security of software:

1. Users should store data, whenever possible, to their default directory which maps to a

corporate fileserver (i.e., f:\private\username)

2. Users of stationary computers should not purposely store data to their computer=s local hard drive. The backup of local hard drives is not the responsibility of the Information Systems Department.

3. Notebook users are responsible for the physical safety of the notebook and the information stored on it. Power-on Passwords may be utilized or the Information Systems can install a third-party application for password protection utilization.

4. If a notebook computer is used outside the bank, data files saved to the local hard drive (C drive) should be re-saved to F:\private\username when the notebook is brought back into the bank. I.S. personnel are not responsible for data backups on local hard drives.

5. For application software with password protection, passwords should be committed to memory and changed at frequent intervals.

Policy #5 - Virtual Security for Corporate Information

The Information Systems Department at Xxxxxxxxxxx protects the bank=s corporate information by effectively detecting and blocking connections from the Aoutside world@ through its T1 Internet connection provided by AT&T. In addition, access to/from outside vendors are forced to communicate through the bank=s De-Militarized Zone on the bank=s firewall. As technology changes, the Information Systems Department proactively searches for new and better ways to prevent intrusion to all new potential points of entry. The services of the International Computer Security Association=s website *(www.icsalabs.net)* is used to alert I.S. personnel to new developments in computer Ahacking@ and as an aid in the reduction of the bank=s network vulnerabilities. Other sources that are utilized by IS personnel include truesecure.com (a reputable vendor of security software), www.sans.org (system administration, networking and security) and www.cert.org (the computer emergency response team coordination center.)

Procedure #5 - Virtual Security for Corporate Information

Border Manager Server - The Internet is considered the bank=s most significant potential point of entry. To offset (and nullify) the risk of outside intrusion, the bank has Novell=s Border Manager installed on a fileserver as a *firewall.* The Border Manager software program utilizes NAT (Network Address Translation) which masks or hides the bank=s internal computers from the Aoutside world.@ All the bank=s Internet users access the Internet via the Border Manager Server, and use NAT.

The Border Manager Server also utilizes packet filtering technology to limit the types of traffic allowed to pass through the firewall. Firewall configuration is accessible by three authorized individuals within the IS Department. The firewall is configured to allow the following types of traffic and/or services:

<u>To/From Internet:</u>
- DNS Resolution
- Web/Secure Web Traffic
- FTP
- ICMP (PING, Traceroute)
- Traffic to/from Vintek (for Loan Ops Dept.)
- SMTP (E-Mail)
- Traffic to/from Fidelity (for Private Banking Dept.)
- NNTP (Net News for Novell=s Support Forums)
- Ports 389, 829 and 700 to specific servers at First Data Resources (for Merchant Services Dept.)

- Traffic to/from RiseSoft (for stock quotes for ticker in lobby)

To/From Vendor DMZ/Internal Network:
- Traffic to/from Ceridian (ASP - payroll/HR)
- Traffic to/from Experian (credit bureau - Consumer Lending)
- FTP Traffic
- Web Traffic

To/From Web-Accessed DMZ/Internal Network:
- Web/Secure Web Traffic
- Web Server Administration Traffic
- ICMP (PING, Traceroute)
- Novell Core Protocol Traffic
- Service Locator Protocol Traffic
- GroupWise Traffic
- IPX Traffic for Administrative Purposes

Border Manager will block all other types of traffic and/or services. As an example, any program that attempts to use other types of services (i.e., Napster, Instant Messaging, etc.) Will not function properly.

In addition, the Border Manager Server has IPX bound only on the internal card for administrative purposes. There is no IPX on the public interface, which prevents any IPX attacks from outside the bank=s perimeter.

WebAccess Server - The WebAccess Server hosts the bank=s GWIA (GroupWise Internet Agent) and our Web Server for web based access to GroupWise. This server is in a DMZ (De-Militarized Zone) with limited exposure to the Internet and is protected by the bank=s firewall.

Vulnerability Testing - The bank utilizes the services of Aimnet Solutions to perform semi-annual vulnerability tests of the bank=s internal network (including the Firewall, the Web Access Server, the Internet Router, the bank=s website and its inventory of modems.) As part of the audit, a comprehensive report is produced that is utilized by I.S. management to ensure that adequate steps are taken to prevent security breaches by hackers and others that might attempt to launch hostile attacks against Xxxxxxxxxxx=s systems.

Intrusion Detection - The bank utilizes a network-based Intrusion Detection System (IDS) by AXENT Technologies, Inc. This system utilizes two separate modules that reside in front of and in back of the bank=s firewall detecting and reporting on common operating system attacks that may come from the Internet or from inside the bank=s environment. Two members of the I.S. team will be trained in the specifics of this system and will be notified (via text-based pagers) should the system detect an abnormality.

Virus Protection - Virus protection is utilized on the Internet Gateway, all bank fileservers and all user workstations and/or notebook PCS. Virus protection is covered thoroughly in Policy #11.

Data Encryption - The bank=s standard for data encryption is PGP (Pretty Good Privacy.) All users are instructed to utilize this technology when sending confidential information as an e-mail attachment. This subject is covered thoroughly in Policy #13.

Retail Branch Servers - Each of the servers in the bank=s retail branch locations has a direct connection to NCR via its frame relay network, creating a possible point of entry at each branch. NCR runs a firewall protecting both themselves and their clients from intrusion.

Modem Pools - The bank utilizes one modem pool as a means to provide a cost-efficient alternative to modem usage. The modem pool utilizes Novell=s Netware Connect product. The modem pool is configured for Aauto-answer = no@ as this modem pool is used exclusively for outgoing calls. Incoming callers, when enabled, are presented with a 1) Netware Connect Password, 2) PC-Anywhere Username and Password, 3) NetWare Username and Password.

Security Breach/
Action Team - Xxxxxxxxxxx believes its data security strategy - via the above-mentioned complement of products and processes - is designed effectively and provides the bank with a secure architecture for customer and employee information.

Should a breach occur, however, the following steps will be taken by the bank=s Emergency Action Team. This team consists of the Chief Operating Officer, the Security Officer and three members of the Information Systems Department.

1) Whatever component of the network that is/was compromised will be immediately turned off and disconnected from the network. A determination needs to be made to see if any other component

of the network was compromised.

2) The most recent backup tape for the effected fileserver/s will be collected because research may indicate that a full or partial system restore is necessary.

3) The server will be built with new/different passwords or PINs.

4) The bank=s Security Officer will be notified, and he will be asked to contact the FBI and the appropriate regulatory agencies to report the breach.

5) Firetower, Inc., the Intrusion Detection vendor/consultant will be notified to assist with the process of tracing the party that infiltrated the bank=s network.

6) Novell, Incorporated will be notified to assist IS management in determining exactly how the Border Manager Firewall was compromised.

7) The Chief Operating Officer will be the liaison between IS management and the bank=s Board of Directors in reporting the incident, the response, the repair and possibly the prosecution of the guilty individual/s.

Policy #6 - Data Backup

Xxxxxxxxxxx=s policy is to backup information stored on corporate fileservers on a daily (i.e., Monday - Friday) basis - or in the case of relatively static servers (i.e., retail branch servers) a weekly backup is required. Weekly backup tapes (from remote locations) are stored at the Records Retention Center at the corporate headquarters for safekeeping. Daily backup tapes from the corporate headquarters are stored remotely at Capital Records - a Providence, RI based firm who specializes in off-site storage of corporate information. Weekly backup tapes are stored at Capital Records for a period of five weeks. Monthly tapes remain at Capital Records for 12 months. The backup software is Seagate=s Backup Exec, and it is configured to perform full-system backups which begin at 7:30 P.M. Backup tapes are not usually retained for longer than one week for most locations. However, significant events such as a routine purges of information, major installations, etc. require that a tape be stored off-site at the Records Retention Center or Capital Records permanently.

Procedure #6 - Data Backup

Backup Procedure

Backup Server Name	Server/s It Backs Up	Frequency	Storage Location
Baker	Baker	Daily	Capital Records
Border	Border, WebAccess	Daily	Capital Records
CMSI	CMSI	Daily	Capital Records
Consumer	Consumer, Groupwise, HRComp, MAG	Daily	Capital Records
Fmark1	Fmark1, Compbank, MAX, SOP	Daily	Capital Records
Fmark 2	Fmark2, Branch01, GL, Operations	Daily	Capital Records
FRMain	FRMain	Daily	Records Center
MVMain	MVMain	Daily	Records Center
PDC	PDC, CiscoWorks, Intranet,		

	Payroll, Rightfax	Daily	Capital Records
PLMain	PLMain	Daily	Records Center
SandMain	SandMain, Mainofc1	Daily	Records Center
*Branches	Each Branch Backs Up Itself	Weekly	Records Center

* All branches except Cape locations.

Backup log files are maintained daily in the I.S. Department and logged to a file. Unusual incidents are immediately investigated and remediated.

Policy #7 - Data Recovery

Backup media may be retrieved from the off-site (i.e., Capital Records or the Records Center) location for the following reasons:

1. A more recent or current backup copy has been made and the copy in remote storage is out of date.

2. A disaster has occurred causing data to be inadvertently destroyed.

3. The data on the backup media is no longer considered to be critical to the operations of the department and/or the bank.

Procedure #7 - Data Recovery

The requested backup media will be retrieved by the Information Systems Department.

If a data recovery routine is being done due to a disaster, the following steps must be taken:

1. The Disaster Recovery Coordinator must be notified that a disaster has occurred.

2. The media must be made Awrite protected.@

3. Once the backup media has been used to recreate the lost data, it must immediately be returned to the off-site location.

Policy #8 - Computer Maintenance/Repair

In order to function as a productive tool, a computer must be maintained in good working order. It is the responsibility of the user to report equipment failures for appropriate corrective action.

Procedure #8 - Computer Maintenance/Repair

When a failure of computer equipment is encountered, the user must follow the proper procedure for reporting the failure and assuring that corrective action is taken:

1. At the time of failure, the user should make every effort to document the failure as clearly and completely as possible.

2. After the failure is properly documented, the user should contact the Information Systems Department (i.e., Enterprise Support Line or the Retail Branch Support Line) and report the failure.

3. The Information Systems Department will place a service call with the appropriate vendor.

4. In instances where the use of the computer is critical to the operation of the bank (typically a retail branch), the Information Systems Department will make reasonable effort to minimize work interruption due to equipment failure by attempting to provide loaner equipment for the user.

Policy #9 - Internet Usage

(This policy is resident in its complete form in Xxxxxxxxxxx=s Personnel Handbook which is issued by the Human Resources Department.)

Internet access to global electronic information resources on the World Wide Web is provided by Xxxxxxxxxxx to assist employees in obtaining *work-related data and technology*. The following guidelines have been established to help ensure responsible and productive Internet usage. While Internet usage is intended for job-related activities, incidental and occasional brief personal use is permitted within reasonable limits.

Procedure #9 - Internet Usage

All Internet data that is composed, transmitted, or received via Xxxxxxxxxxx is subject to disclosure to law enforcement or other third parties. Consequently, employees should always ensure that the business information contained in Internet E-Mail messages and other transmissions is accurate, appropriate, ethical, and lawful.

In an effort to maintain a workplace free of harassment, the bank uses CyberPatrol software to *block access* to Internet sites categorized as: Violence/Profanity, Partial Nudity/Art, Full Nudity, Sexual Acts& Text, Gross Depictions/Text, Racist/Ethnic Impropriety, Satanic/Cult, Drugs/Drug Culture, Militant/Extremist, Quest/Illegal/Gambling.

The equipment, services, and technology provided to access the Internet remain the property of Xxxxxxxxxxx. *Xxxxxxxxxxx reserves the right to monitor Internet traffic, and retrieve and read any data composed, sent, or received through its online connections and stored in its computer system.*

Policy #10 - E-Mail Usage

(This policy is resident in its complete form in Xxxxxxxxxxx=s Personnel Handbook which is issued by the Human Resources Department.)

Xxxxxxxxxxx strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, Xxxxxxxxxxx prohibits the use of computers and the e-mail system in ways that are disruptive, offensive to others, or harmful to morale.

Procedure #10 - E-Mail Usage

The bank=s E-Mail System (GroupWise) may not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters.

While E-Mail usage is intended for job-related activities, incidental and occasional brief personal use is permitted within reasonable limits.

The equipment, services, and technology provided to access the E-Mail System remain the property of Xxxxxxxxxxx. *Xxxxxxxxxxx reserves the right to monitor E-Mail traffic, and retrieve and read any data composed, sent, or received through its online connections and stored in its computer system.*

Policy #11 - Response to Computer Viruses

It is Xxxxxxxxxxx=s policy to install virus protection on all corporate computers - at all points of entry. Currently those points of entry are: Fileservers, Internet Gateway and Workstations.

Fileservers - Mcafee=s Netshield is running on all corporate fileservers as an NLM (Network Loadable Module.) Virus detection files are kept current via Mcafee=s backweb technology on Enterprise Fileservers. Retail Branch Fileservers are kept current by a manual copy of the most recent virus detection file. If a virus is detected, the network supervisor is notified.

Internet Gateway - Guinevere (from Indecon), a Novell partner, is installed on the Internet Gateway on the Groupwise E-Mail Server. It scans incoming and outgoing E-Mails (and attachments) for viruses and Areturns to sender@ any message with an infection. The intended recipient is notified that a message and/or attachment addressed to them was infected, detected by Guinevere and returned to the sender. If a virus is detected, the network supervisor is notified.

Workstations - Mcafee=s Vshield is running on all corporate workstations. The Vshield version and virus detection files are kept current via a program developed by Mcafee. This program file is E-mailed to users with instructions as to how to execute the program.

Users are required - as outlined in Users Responsibilities - to notify a member of the I.S. team is a virus is detected.

Procedure #11 - Response to Computer Viruses

1. Users should immediately cease to use the computer on which the virus is detected. Power the computer OFF.

2. Contact the Information Systems Department immediately.

3. The Information Systems Department will take appropriate corrective action to include a quarantine of the suspect system and the use of Avaccine@ software.

4. The Audit Department will be notified of the incident and any corrective action that was taken.

Policy #12 - User Support

In order to maximize the bank=s investment in technology, the Information Systems Department strives to maintain a high level of customer support to its userbase. User support is separated into two distinct sections (i.e., Retail Branch Support and Enterprise Support.) Key fields of information related to support calls (i.e., verbal or written) are logged into a database, and the amount of time it takes to resolve an issue is analyzed. This analysis is conducted in an effort to provide a thorough and quick resolution to support issues on an on-going basis. Both support groups within the Information Systems Department have others within the department who can be consulted to assist in solving user support issues.

Procedure #12 - User Support

The Retail Branch Support Group within the Information Systems Department consists of two individuals whose focus is supporting the bank=s 40 retail branch locations. These individuals are well-versed in the hardware and software utilized throughout the retail branch network and communications issues related to the bank=s data processing center.

A support call is initiated via a telephone call to the Retail Branch Support Line. If the call is not answered after three telephone rings, the bank=s internal phone system automatically generates a call to a pager belonging to the Retail Branch Support Group. This system was implemented due to the fact that most support issues emanating from retail branches require immediate assistance. Support calls are resolved via telephone - if possible - but site visits are routinely conducted if the problem cannot be remediated over the phone. Retail Branch Support personnel wear their pagers during the evening and weekends in the event that branch personnel require assistance during extended hours. If retail branch personnel require assistance with an issue that does not need immediate attention - users are instructed to utilize the Information Systems Department=s Request for Services Form. Under most circumstances, critical support issues within the retail branch network are resolved immediately. Non-critical issues are resolved within one week.

All users outside of the retail branch network are serviced by the Enterprise Support group within the Information Systems Department. These two individuals are well-versed in the numerous applications that support both back-office and front-office users and communications issues related to the bank=s data processing center.

A support call is initiated via a telephone call to the Enterprise Support Line. If both support personnel are unavailable, users are instructed to leave a voice mail message. Both Enterprise Support personnel publish their pager numbers on their voice mail message, and encourage users to page them if the issue is critical. In addition, these support personnel wear pagers during the evening and weekend hours in the event that assistance is needed during extended hours. If assistance is required with an issue that does not need immediate attention - users are instructed to utilize the Information Systems Department=s Request for Services Form (Exhibit A.) Under most circumstances, critical support issues handled by the Enterprise Support Group are resolved immediately or within one day. Non-critical issues are resolved within one week.

Policy #13 - Data Encryption

The use of data encryption methodology is required by all users who send confidential information as an e-mail attachment over the Internet. Confidential information is defined as that information that is *nonpublic personal information* - or information which can personally identify a customer or an employee.

The Internet is not yet a totally secure environment. To mitigate this risk to the bank=s customer and/or employees, the use of data encryption technology is required. Data Encryption ensures authenticity and establishes communication in a way that prevents anyone (other than the intended addressee) from accessing the encrypted information.

The bank=s standard for data encryption is PGP (Pretty Good Privacy.) PGP is based on the industry-standard RSA methodology for encryption and decryption via a pass-phrase.

Procedure #13 - Data Encryption

When sending confidential information as an e-mail attachment over the Internet, be sure to utilize PGP. Please refer to the specific instructions that you received from the I.S. Department. Or, call I.S. personnel and they will install the software and instruct you on how to utilize it. Your passphrase should be chosen at random and be difficult to Acrack.@

Policy #14 - Local Area Network (LAN) Access

It is the policy of Xxxxxxxxxxx to grant access to the LAN and its applications only if requested by an authorized Department Manager. This request must be made in writing or electronically and must be signed by the appropriate Department Manager. Information Systems support personnel will not fulfill a request for LAN access unless the request is made in writing using either the Network Access Form (for non-retail branch personnel - Exhibit B) or the Request for Services Form (for retail branch personnel - Exhibit A.)

Procedure #14 - Local Area Network (LAN) Access

When requesting access to Xxxxxxxxxxx=s network, a Department Manager must complete either a Network Access Form or a Request for Services Form and forward that document to the appropriate support personnel (i.e., enterprise support or retail branch support) in the Information Systems Department.

The Network Access Form is a comprehensive document designed to meet the needs of non-retail branch personnel and their diverse computer requirements. The Request for Services Form is more generic in design and satisfies the needs of retail branch personnel whose access to the network is typically limited to the teller/platform system and/or word processing and e-mail if the user is located in the platform area.

Upon receipt of the Network Access Form, a copy is forwarded to the Compliance/Security Department so the appropriate NCR STARCOM/CIS codes can be issued (i.e., inquiry only, maintenance capabilities or financial capabilities) directly to the user.

For retail branch personnel, teller numbers and access codes are requested from the Compliance/Security Department by the Teller Training Officer prior to permanent placement with a retail branch.

When an employee is terminated or he/she resigns from Xxxxxxxxxxx, the Human Resources Department issues a Network Access Delete Form for Terminated Employees (Exhibit C.) This form is immediately forwarded to the Information Systems Department, and this user is deleted from the bank=s network system.

Xxxxxxxxxxx
Third Party Applications/Programs - Risk Assessment

Overview:

Risks associated with the bank=s third-party applications are reviewed annually by the I.S. Manager and the appropriate business unit managers. Access to (and removal from) 3rd party applications are kept current via cooperation between human resources personnel, IS personnel and the 3rd party application administrators (see Exhibits D and E - forms utilized to remove or re-evaluate users and access to particular third-party applications.) Risks are minimized by the bank=s use of various electronic and physical safeguards that seek to protect all network applications from internal and/or external threats. These safeguards are outlined - in detail - in the bank=s Information Systems Policy and are included in the bank=s Information Security Program (which is an addendum to the bank=s Privacy Policy.)

Electronic safeguards include daily off-site storage of system backup tapes and optical disks, data encryption, virus protection, a secure firewall, semi-annual penetration testing against the firewall, an intrusion detection system and an Emergency Action Team. Control over PCS with local modems is maintained via quarterly hard drive scans. In addition, I.S. management regularly reviews Network Operating System Security Reports (i.e., both third-party and system generated.)

The bank utilizes three network operating systems. They are Novell, WindowsNT and UNIX. They are kept current by implementing the latest, proven operating system enhancements. Novell and Windows NT are configured to require unique system usernames and passwords. User passwords must be eight characters in length and users are required to include one number and one special character in their password. Users are prompted and required to change passwords every 60 days. The UNIX system requires at least six characters in its password, and users are required to include one number. The UNIX system is configured to require password changes every nine weeks (63 days.)

Physical safeguards include proxy card access, secure cabinets and locking files in which documents are stored. Disposable confidential information is picked up by Data Destruction Services, a bonded company.

Individual Assessments:

Baker Hill

Classification = Important:

Two components of the Baker Hill One Point suite of software are licensed and utilized by Xxxxxxxxxxx. They are STAN and REACT. STAN automates financial analysis and projections, while REACT is used for exception tracking. The Baker Hill application resides on a Novell Network Server and is accessible to members of the Commercial Loan and Credit Administration Departments and a few other users throughout the bank. Commercial lenders are located at each of the bank=s regional locations (i.e., Corporate Headquarters, Fall River Central, Plymouth Central, MV Central and Cape Central) and access to the database (which is stored at the Corporate Headquarters) is made accessible via the bank=s Enterprise Wide Area Network.

Baker Hill contains non-public, personal information (i.e., social security numbers, loan and deposit accounts numbers, financial information, credit information and income information) relative to the bank=s commercial borrowers.

The Baker Hill One Point application is administered by the Credit Administration Officer, Renee Vallee. Usernames and passwords within Baker Hill are automatically synchronized with the Novell Operating System. Therefore, usernames and passwords are unique and users are prompted and required to change their passwords every 60 days. Within the STAN and REACT modules of Baker Hill, security is further enhanced via the use of user profiles. User profiles are determined by the management of the Credit Administration Department and maintained by the System Administrator, Renee Vallee. Only three Xxxxxxxxxxx employees maintain supervisory access to this application. They are Renee Vallee, Credit Administration Officer, Bruce Lemieux, SVP - Credit Administration and Susan St. Pierre, Team Leader of Enterprise Support within the I.S. Department.

Credit Revue

Classification = Important:

The Credit Revue application is a UNIX-based solution (utilizing a Progress Database) which Xxxxxxxxxxx licenses from First American/CMSI to automate the processing and decisioning of its consumer loan products. The Credit Revue system is used extensively throughout the bank=s Consumer Loan Department. Access to Credit

Revue is limited to members of the Consumer Loan Department. The Database Administrator, Debra Sewell of the I.S. Department, maintains access to the Progress Database but does not have access to the Credit Revue system=s production module. She does maintain full access to the test module.

Credit Revue contains non-public, personal information (i.e., social security numbers, loan and deposit accounts numbers, financial information, credit information, income information and the results of credit reports) relative to applicants of the bank=s consumer loan products.

The administrator of the Credit Revue system is Jim Malinowski, VP of Consumer Lending. Bill Rigby, SVP of Consumer and Donna Oliveira, AVP of Consumer Lending also maintain supervisory access to Credit Revue. Jim Malinowski is charged with establishing user profiles within the various modules (i.e., Loan Admin, Credit Processing, Reports, Report Writer, Maintenance and Utilities.) User profiles are dictated by job responsibilities. Users are prompted for password changes every 90 days. Passwords must be at least eight characters in length with at least one number.

Fin/ess
Classification =
Critical:

The bank utilizes the Fin/ess General Ledger System which is licensed software from First National Systems (FNS) out of Cotuit, Massachusetts. This system includes all aspects of General Ledger accounting including Fixed Assets, Accounts Payables and Safe Deposit Box modules. It resides on a Novell Network Server. The database engine utilized is Synergy which is also licensed from FNS. The System Administrator, Matt Sylvia (VP - Financial) checks annually with FNS to ensure that the latest version of the software code is stored in escrow. Primary users of the Fin/ess system are within the Financial Division. However, Loan Operations and Deposit Operations also maintain limited access. Still others maintain Aread only@ access to some General Ledger Reports.

Fin/ess contains confidential, financial information regarding the bank, its subsidiaries and the holding company, Seacoast Financial Services. In addition, Fin/ess stores non-public information as it relates to those customers with safe deposit boxes (i.e., name, address and corresponding account numbers.)

Three members of the Financial Division maintain supervisory access to the Fin/ess system. They are Frank Mascianica, EVP; Matt Sylvia, VP and Diane Farnworth AVP. The administrator of the system is Matt Sylvia. User profiles - based on job responsibilities - are determined by Matt. Separate profiles exist for each of the various companies in Fin/ess (i.e., the bank, the bank=s subsidiaries, the holding company and its subsidiaries.) Unique usernames and passwords are utilized. Passwords must be a minimum of 8 characters in length and users are prompted and required to change passwords every five months.

Ceridian

Classification = Important:

The Ceridian Source 520 HR/Payroll system integrates human resources and payroll functionality. This application is licensed by the bank from Ceridian Corporation and is configured to be accessible to members of the Human Resources Department only. It is installed on a WindowsNT server and its database engine is Microsoft Access.

The Ceridian system contains confidential information regarding the bank=s employees, former employees and applicants (including social security numbers, compensation information and other confidential information.)

The Ceridian system is administered by the Human Resources Officer, Susan Baptista. Those with supervisory access to the system include Linda Empoliti, VP of HR; Susan Baptista, HR Officer and Paula Pinarreta who is responsible for payroll processing for the bank. Usernames and passwords within Ceridian are automatically synchronized with the WindowsNT operating system. Therefore, usernames and passwords are unique, and users are prompted and required to change their passwords every 60 days. Security is further enhanced via the use of user profiles within the system. User profiles are dictated by job responsibilities and assigned by the system administrator.

Express Options

Classification = Important:

Express Options is licensed software the bank utilizes to manage its Stock Option Program. It resides on a Novell Network Server and utilizes a Pervasive SQL Database Engine. Access to this program is limited to members of the Human Resources Department, the Financial Division and the Marketing Department (for investor relations reporting.)

Express Options contains confidential information as it relates to those Directors and Officers who participate in the bank=s Stock Option Program. Compensation information as well as social security numbers are stored in this system.

The administrator of Express Options is Susan Baptista, HR Officer for the bank. She maintains supervisory access to the system along with the VP of Human Resources, Linda Empoliti. Users within the Marketing Department and the Financial Division maintain Aview only@ access to specific reports generated by the system. User profiles are established and maintained by the System Administrator. The system does not automatically prompt users for password changes, therefore this task is assigned to the System Administrator. Unique passwords are assigned to the users every ninety days. Passwords are eight characters in length (with one number being part of the scheme.)

Mortgage Management

Classification = Important:

The Mortgage Management system is licensed software from Sound Software which is used by the bank to originate, process and close its residential mortgage loans. The program resides on Novell Network Servers at each of the bank=s regional locations. The database resides at the corporate headquarters, and information is accessed via the bank=s Enterprise Wide Area Network.

The Mortgage Management system contains non-public, personal information (i.e., social security numbers, loan and deposit account numbers, financial information, credit information, income information and the results of credit reports) relative to applicants of the bank=s residential lending portfolio.

The Mortgage Management System is administered by Donna Medeiros an Assistant Vice President in the Lending Administration Department. She and her assistant, Priscilla Nutter, maintain supervisory access to the system. Users are assigned unique usernames and passwords every 90 days by the system administrator. Passwords are at least 8 characters long and utilize 7 letters and 1 number. User profiles are determined based on job responsibilities (i.e., managers, underwriters, originators, processors and loan closers) and configured by the system administrator.

CARM

Classification = Important:

The Collections and Asset Recovery Management System is licensed software from Intelligent Banking Solutions (IBS) utilized by the bank

which streamlines the delinquent loan collection process. It is used exclusively by the Managed Assets Group, and is administered by the bank=s Vice President of the Managed Assets Group, Wayne Carvalho. CARM resides on a Novell Network server. Each morning a routine is executed where xxxxxxxxxxx obtains a file of delinquent accounts from the data processing center=s FTP server. This file is then indexed into CARM.
CARM contains non-public, personal information (i.e., social security numbers, loan account numbers, credit information, results of credit reports and confidential narratives between customers and collectors) relative to the bank=s delinquent loan customers.

For most members of the Managed Assets Group, access to various loan portfolios is segmented and based on job responsibilities. Management and administrative personnel within MAG maintain the ability to access all loans regardless of portfolio segmentation. Users are instructed to change their passwords every 90 days. They are instructed to choose a password which utilizes 8 characters (seven letters and one number.) Because the system administrator maintains a list of all user passwords, he ensures that password changes are made timely and in line with the bank=s standards.

Max$ell

Classification = Important:

The Max$ell MCIF system is licensed software from Harland Corporation utilized by the bank=s Marketing Department. The Max$ell MCIF system receives monthly updates of customer information from the bank=s data processing center (via CD-ROM) and is regularly complemented with demographic information relative to the bank=s customers. Max$ell resides on a Novell Network server.

Max$ell contains non-public, personal information (i.e., social security numbers, loan and deposit accounts numbers and various other pieces of customer and account information) that correspond to the bank=s entire customer base.

The administrator of the Max$ell system is the Marketing Officer, Monica Spach. She maintains supervisory access to the system along with Jim Rice, SVP - Marketing and Susan Nelson, AVP - Marketing. Unique usernames and passwords are assigned and established by the System Administrator with expiration dates equal to 90 days. The system prohibits numerical data within its password routine. Passwords lengths are a minimum of eight characters.

SMARTi
Classification =
Important:

The SMARTi system is licensed software from Filemark Corporation. The bank utilizes this system for COLD storage of its core processing reports from the NCR Starcom system, reports generated by the bank=s ATM processor and reports generated by the bank=s items processor. SMARTi utilizes a Sybase SQL database engine and the databases and COLD reports resides on Novell Network Servers. All data is Aread-only@ and stored using a combination of hard disk storage on the bank=s fileservers and WORM (write-once-read-many) disks housed in Hewlett Packard juke boxes. This application is available to various users throughout the bank - primarily in Deposit Operations and Loan Operations.

SMARTi contains non-public, personal information (i.e., social security numbers, loan and deposit account numbers and other account information) relative to the entire customer base.

The administrator of the SMARTi system is Debra Sewell, Database Administrator within the I.S. Department. Several members of the I.S. Department maintain supervisory access to the system. Most reports are available to all users of the SMARTi System. However, some reports - as deemed confidential by bank management - are restricted to those users whose job responsibilities require access to such information. Subsequently, those select users maintain a unique password to the system which is changed every 90 days by the System Administrator. Passwords are eight characters in length and contain one numeric character.

Branch Management System
Classification =
Critical:

The Branch Management System (or BMS) is licensed software from the bank=s core processor, NCR Corporation. This software is used extensively throughout the retail branch network. It provides teller and platform functionality in a DOS-based environment. Each branch has a gateway PC which is directly connected to a 9.6 channel on a 56kb line to pass transactions to the host (i.e., NCR.) There is one Asuper@ password for BMS, and this password is owned and maintained by the I.S. Department. (This does ***not*** mean that the I.S. Department can gain access to the host, however. It simply means that the I.S. Department has full functionality within the software.) This password is changed every six months by I.S. personnel. It is a labor-intensive process as each branch fileserver must be remotely accessed to change this password. This

Asuper@ password is required when updates are made to the software.

Each branch manager is responsible for setting up his/her staff members with the appropriate level of access (i.e., manager or teller) within the software. Signing in locally and signing in to the host system is made possible via teller numbers and passwords. Teller numbers are assigned by the Security Officer while the teller is enrolled in a teller training class. Passwords are chosen by the user. The system does not periodically prompt users for password changes - nor can it be configured to do so.

Outside of the retail branch network, there are a few other bank employees who utilize the BMS system for financial transactions. Access to BMS must be authorized, in writing, by the Department Manager.

Micro-upload

Classification = Important:

Micro-upload is licensed software from Integrated Software Solutions, which is a partner of the bank=s core system provider, NCR Corporation. It is used by the bank=s Mortgage Lending, Consumer Lending, Loan Operations and Deposit Operations Departments. Access to the NCR host via Micro-upload is controlled by teller numbers - which are issued by the bank=s Security Officer. Micro-upload is installed only on select PCS with unique terminal numbers. Transactions performed can be traced back to a particular terminal and teller via NCR=s Terminal Proof Report. Access to the Micro-upload software and the appropriate level of teller access is requested in writing by the Department Manager.

(3rdprty.wpd)

Appendix A

Recommended Equipment

Fileservers:

1. Compaq (latest model available) with Raid 5 and redundant power supplies.

Desktops/Notebooks:

1. Compaq P4 or latest model available
2. Compaq P3 or latest model available

Monitors:

1. NEC 17" Color SuperVGA

Printers:

1. Hewlett Packard (various models)

Modems:

1. Hayes 56kb
2. Xircom 56kb (for notebook PCS)

Appendix B

Recommended Software

Network Operating System

1. Novell Netware Version 5.1

2. Windows NT 4.X or Windows 2000 (typically driven by application vendor)

Workstation Operating System

1. Windows 98

Data Base Management

1. Microsoft Access for clients

2. Sybase or Oracle for servers

Presentations

1. Microsoft Powerpoint

Spreadsheet

1. MS Office 2000 - Excel or Lotus Millennium

Wordprocessing

1. MS Office 2000 - Word or Wordperfect (version 6.1/8.0)

Graphics

1. Microsoft Powerpoint

2. Harvard Graphics

Flowcharting

1. Visio 2000

Computer Diagrams

1. Visio 2000

Virus Protection

1. Mcafee (server & desktop)

Backup Software

1. BackupExec (server)