# Technology Risk Management policy [1]

[1: This model policy provides the underlying basis for an integrated policy to manage the transaction, strategic, and reputation risks inherent in electronic banking in today’s technological environment. It serves as the umbrella” for separate, specialized policies as described in the section "Scope” below.]

## Bank Name [2]

[2: Your bank name should appear on the policy to clearly indicate to users and regulators that it is your bank's statement of policy, not a generic policy that purports to fit every bank.]

## Purpose

Technological advances are rapidly changing the way banks conduct their business and the very nature of that business. The benefits of these advances include more efficient methods for maintaining and processing data and new methods for communicating with customers and delivering products and services to them. At the same time, this technology involves:

* The traditional physical and environmental risks, such as insider attacks, fire and water damage, theft, and physical damage.
* Newer and potentially more dangerous threats from cyber-criminals, involving unauthorized access to customer or bank funds or data, and cyber‑terrorists, with the threat of using tools such as computer viruses and ransomware.

The board of directors is responsible for the overall supervision of the bank, including the deployment and effects of electronic technology. This policy is intended to assist the board, and thereby the senior management and staff of our bank, in carrying out this responsibility and managing the risks associated with this technology.

## Objectives

This policy is designed to identify the risks inherent in electronic banking, and establish the parameters for the general scope and use this bank will make of electronic technology, the process for planning and implementation of it, and the responsibilities and safeguards for its implementation, use, and risk management.

## Scope

This policy addresses our bank’s consideration and overall use of all aspects of electronic communications and banking. This general policy establishes the parameters for and is supplemented by subordinate policies covering specific aspects of technology and electronic banking, including**: [3]**

[3: Adapt the following list, and develop the necessary policies, to reflect those technologies and/or systems which your bank presently employs or is likely to adapt in the near future.]

* Electronic funds transfers between our bank and other financial institutions, whether initiated by telephone, direct access to Fedline, or other electronic or telecommunications systems.
* Electronic banking systems which directly link the customer with the bank through the Internet, or any other method of remote connection, including internet or mobile banking and ATMs.
* Electronic data processing.
* General use, on bank computers or systems, of intranets (includes local area networks (LANs) and wide area networks (WANs)) and the Internet. This includes email and other collaborative and research tools.

## Risks and Concerns

All of these technology-related applications, to one degree or another, share common risks and concerns, including:

* The maintenance of accurate and complete records.
* Physical protection of data from internal and external hazards.
* Customer privacy rights, expectations, and regulations.
* Appropriate use of bank equipment and software by employees.
* Contingency planning and procedures for backup or reconstruction of bank records.
* Audit procedures to test and confirm the adequacy of protection against these risks and concerns.
* Procedures for reporting status and activities to senior management, the board of directors, and regulatory and law enforcement authorities.

## Our Approach to Technology [4]

[4: This section is intended to set forth your bank's attitude or philosophy regarding its approach to electronic banking. You must adapt and write this section specifically for your bank. The following three different possibilities are given only as examples to assist you in describing your bank's policy.]

1. Because of the costs, potential risks, and our perception of our customer base, it is the policy of this bank to move slowly and cautiously into new areas of electronic banking. Additional internal information-only systems will be considered and adopted when the demonstrated benefits will outweigh the costs. External systems of all types directly involving customers will be considered in light of the local competitive situation and will be adopted only when the costs arising from probable loss of customers is expected to exceed the cost of establishment of new systems.
2. It is the policy of this bank to keep pace with our competitors, but not be a leader, in the use of electronic banking systems. Internal information systems will be enhanced as it appears that the advantages of doing so will be in the bank's long-term interest and within its financial and budgetary capabilities. Expansion of the Internet site or the adoption of other forms of electronic banking will receive ongoing consideration in light of customer desires, competitive pressures, costs and benefits, and risk management factors. In short, we intend to remain competitive but not on the leading edge of electronic banking.
3. It is the policy of this bank to be a leader within our market area in the development and offering of advanced technological services when and where it is economically feasible to do so. Internal information systems will be enhanced to enable the bank staff to more effectively serve our customers, cross-sell services to existing customers, and attract new customers. Our Internet site will be expanded to accommodate electronic banking services as soon as it is economically feasible to do so, and the services can be provided with the necessary degree of security. In the same manner we will continually explore and consider the adoption of additional technological services that have the potential to provide new services to our customers and profits to the bank.

## Responsibility and Management Structure [5]

[5: This section should be amended as necessary to fit your bank's structure and situation. It is essential, however, that the policy specifically assigns responsibility at both the oversight and operational levels. This model policy describes a committee structure that includes representation of senior management, planning and budgeting, operations, marketing, and risk control. By way of comparison, a similar organizational structure, in the form of an asset/liability committee (ALCO), has been effective in many banks for that area of risk management responsibility.]

The board of directors is ultimately responsible for the bank's use of electronic technology and the effects of that use. Ongoing management of the process, however, is delegated to the president **[6]** with the advice and support of the Technological Services Committee (TSC**) [7]** and the Technology Security Officer (TSO**) [8].**

[6: If the delegation of authority is to an individual other than the president, make the appropriate change here. It should be, however, someone at the senior management level.]

[7: You may prefer a different name for this group; if so, make the appropriate change here and wherever its name (usually abbreviated as "TSC") appears later in this model policy. It is suggested, however, because of the unique nature and level of responsibilities of the group, that this responsibility not be simply added to an already-existing group in your bank.]

[8: This listing of a TSO assumes that your bank adopts the management hierarchy stated in this model policy. Additionally, you may wish to use this basic structure but have a different title for the position.]

## Technological Services Committee (TSC)

### Committee Objectives

The TSC brings together all major stakeholders in the bank's electronic technology process and serves as the bank's primary advisory body in this regard. It thereby enables the bank to achieve both control and maximum advantage from technology, considering costs and benefits to both internal and external users, broadening of our customer base, and risk control.

### Committee Membership and Structure

The TSC will be chaired by the president, or the cashier in the absence of the president. The cashier will be the secretary of all committee meetings and will maintain minutes**. [9]** Other voting members of the committee are**: [10]**

[9: The situation of the president acting as the chair and the cashier acting as secretary may be typical for many banks. However, this paragraph should be changed as needed to fit your bank's situation.]

[10: Change the membership list to fit your bank's situation. The objective is to have representation on the committee from all parts of the bank which will be affected by the committee's decisions.]

* Vice president in charge of operations
* Chairman of the planning and budgeting committee
* Technology Security Officer (TSO) **[11]**
* Manager of computer services and programming
* Manager of customer services operations
* Branch manager representative
* Marketing officer
* Internal auditor
* An outside director (rotating position) **[12]**

[11: See the discussion below as to this and alternative positions.]

[12: Having directors serve on this committee on a rotating basis is suggested for two reasons: (1) it provides for direct liaison between the committee and the board; and (2) it can be a valuable learning experience for the directors.]

The committee makes recommendations to and receives the approval of the president before implementing recommendations. Major changes or initiatives will receive approval of the board of directors before implementation.

The committee will meet on call, but at least  . **[13]** Appropriate minutes will be kept and presented to the board of directors.

[13: Insert the frequency of meetings. Monthly meetings will be common for many banks, but if a different meeting interval is appropriate for your bank, state it accordingly.]

### Committee Duties

The TSC will perform the following duties as they pertain to the bank's electronic systems and planning: **[14]**

[14: This is a suggested list of practical duties. Add or delete suggested items to fit your bank’s situation.]

* Maintain, update, and review a comprehensive list of all technology projects proposed and in progress.
* Review existing systems for effectiveness and obsolescence, and make recommendations as appropriate regarding changes or enhancements to them.
* Conduct, review, and update strategic and shorter-term plans regarding systems, including likely costs and benefits.
* Review and make recommendations regarding the security, privacy, audit, and legal aspects of the bank's existing or proposed new systems.
* Review and make recommendations regarding proposed vendors, outsourcing, and contracts prior to their adoption.
* Monitor competitive developments that affect our bank's position and incorporate these factors into the planning process.
* Review and assess the level of customer satisfaction and usage of our bank’s technology-based products and services.
* Review marketing material, prior to its use, as it pertains to electronic services.
* Review and coordinate contingency planning as it involves electronic systems with those persons or groups **[15]** responsible for bank-wide contingency planning.
* Coordinate with and oversee the activities of the Electronic Data Processing Committee**. [16]**
* Report monthly to the board of directors as to recommendations and significant developments.

[15: Rather than referring to "those persons or groups” you may prefer to identify them by title or name.]

[16: If your bank has an existing policy and/or a specified group or individual responsible for EDP activities, it is important to eliminate any conflicting areas of activity, responsibility, or authority.]

## Technology Security Officer [17]

The Technology Security Officer (TSO) is responsible for the overall coordination and day-to-day operation of the bank’s technology risk system. The TSO is to be appointed by the bank president with confirmation by the board of directors, and reports to the president. **[18]** The TSO has full access to all bank systems and all systems administrators will defer to the TSO in matters of security. The TSO’s responsibilities include the following**: [19]**

[17: This assumes you are using the management hierarchy suggested in this model. If that is not your choice, make the necessary changes here. If you are electing to use the model, but with a different title, make that title change here and wherever TSO appears later in this model policy. As an alternative, your bank may wish to consider the concept of a Chief Information Officer (CIO), a position used in a variety of business organizations. A CIO typically would be at the same level as a bank’s Chief Financial Officer and would have a broad range of responsibilities, being in charge of all of the bank’s information systems and technological efforts, such as acquiring new computer systems, e-commerce, Internet presence, etc.

[18: Make such changes in this sentence as are needed to fit the appointment process and reporting lines to be used in your bank.If you adopt the CIO option, above, the TSO would report to the CIO, or the TSO’s duties as stated in this model policy would be incorporated into the CIO’s duties.]

[19: This is a suggested list of duties. Add additional or delete suggested items to fit your bank’s situation.]

* Implement, manage and enforce the bank’s information security and cybersecurity program
* Provide an annual information security program status report to the board, and provide more frequent security reports or notifications as needed
* Oversee the bank’s information security and cybersecurity training initiatives for employees and the Board
* Oversee annual reviews of user access within the bank’s information systems
* Oversee the development and ongoing management of the information security risk assessment
* Oversee the development and ongoing management of the cybersecurity assessment
* Participate in the initial and ongoing evaluation of the security controls implemented by the bank’s vendors
* Work with business line managers to understand new initiatives, evaluate the inherent information security risk of these initiatives, and outline ways to mitigate these risks
* Work with business line managers to understand the flows of information, risks to the information, and ways to protect the information
* Monitor system security reports to identify and investigate exceptions or potential malicious activities
* Monitor threat intelligence services (FS-ISAC, CERT, etc.), regulatory press releases and other industry news to stay abreast of current threats and regulatory requirements
* Maintain the bank’s incident response plan and serve as the leader of the Incident Response Team
* Provide documentation for independent audits of the bank’s information security and cybersecurity program
* Other duties and responsibilities as assigned by the president, the TSC, or the board of directors.

The TSO’s duties pertain to technology security, not technology operations. Ambiguities, misunderstandings, or disagreements between instructions or interpretations issued by the TSO and the head of an operating division will be resolved by the TSC.

### Planning

Because of the rapid changes in electronic banking technology, it is recognized that it is virtually impossible to develop a detailed long-term plan. However, the significance of electronic banking, particularly as to its costs and benefits, make it essential that there be a thoughtful planning process. The TSC will, therefore, develop and update as needed a conceptual plan covering a rolling three-year time period **[20]** for electronic banking services. This plan will be coordinated with and integrated into the bank's overall strategic plan with respect to when, where, and how the bank will provide technology-based services to its market area.

[20: A three-year period for the plan can provide a basis for budgeting and implementation for the current and following years. You may, however, wish to change the planning period to fit your bank's practices and needs. It is recommended that the plan be continually updated in light of known changes and be extended each year so that it continually covers the intended future year or other time period.]

### Budgeting

The TSC will develop budget information and provide it in a timely manner to be integrated into the bank's overall annual budgeting process. This budget information will include data on both costs and income, taking into consideration estimated costs and marketing and pricing expectations.

### Implementation

The TSC will oversee the implementation of significant electronic banking initiatives and make periodic status reports to the board of directors. New systems will not be put into full operation, although limited test runs may be conducted, until the TSC and the board of directors are satisfied that the system will meet expectations as to operational quality, safety and privacy concerns, other risk management considerations, and audit standards.

## Security Concerns and Safeguards

Threats or damage to the integrity of the bank’s computer systems or the data contained within them can come from either internal or external sources. Our overall approach to technological security is a layered system which builds upon and links to the other layers. These layers consist of:

* Written policies and operating procedures.
* Physical security measures.
* Personnel security measures.
* Computing and data base security measures.
* Audit trails and detection measures.
* Reporting requirements and procedures.

As tools to implement these layers of risk management, the following minimum safeguards will be employed for all computer-based systems and operations.

### Policies and Operating Procedures

This Technology Risk Management Policy will be supplemented by written operating procedures to be developed, updated, and maintained by the TSC and TSO**. [21]**

[21: As is common with most management policies, this model policy spells out the “what” that is to be done. Written procedures are essential to detail the “how” aspect. These procedures will typically be written by or within the bank’s operating section to which the procedure applies, but subject to the approval and oversight of the TSC.]

### Physical Security

It is necessary that our computers and related equipment be protected from physical damage or tampering. Procedures and measures to accomplish this include**: [22]**

[22: These are commonly used measures to protect computers and computer systems. You may wish to amend these suggested items or add others. Remember that adequate physical security is an essential part of risk management, even though it may be regarded as “inconvenient” or “unnecessary” to some people.]

* Primary equipment, such as servers and networking equipment, should be located in a separate room(s) with the door locked at all times.
* Access to these locked rooms is limited to personnel who have both a need and the clearance to be there.
* Access to freestanding computer or related equipment within the bank is to be restricted to authorized users, enforced by password and/or physical lock and key protection.

### Personnel Security

The ultimate threat to computer security is the insider, either through innocent errors, which may result from carelessness or improper training, unwitting or intentional introduction of malicious programs, or intentional harm.

We will employ, at a minimum, the following measures to protect the bank’s equipment, data , and the employees themselves**: [23]**

[23: This list is not necessarily all-inclusive. These suggestions are, however, basic elements in an adequate protective system. Care should be taken, if any of them are to be deleted in your bank’s policy, that alternative protective measures be included.]

* Users and the levels of use are to be authorized specifically by name by the TSC or TSO.
* Security clearance checks, with periodic updating, are required for all personnel designated as being in security-sensitive positions.
* Access to any bank computer system is to be controlled by use of a unique password for each authorized user. Passwords are to be changed monthly and should be of a nature not easily duplicated or broken by unauthorized users. Written procedures and training will be instituted to discuss proper password usage, such as mixing alpha, numeric, and special characters, avoiding dictionary words, etc. Employees are to be reminded on an ongoing basis that passwords are vitally important in the protection of the bank’s systems and data and this importance outweighs any inconveniences that may be encountered or perceived regarding the use of passwords. **[24]**

[24: An effective password system depends on the cooperation and participation of the users. It is therefore important that employees be kept aware of both the need and the process.]

* In addition to the access controls stated above, access to and use of bank data is limited to a "need to know" basis. Customer information, or other types of bank data, must not be used for other than official purposes. Written standards and employee training will be utilized to communicate these standards.

### Computing and Data Security

All technology risk management procedures and safeguards addressed in this policy ultimately focus on one paramount concern: the integrity of the bank’s data. The following procedures, one part of our layered system, directly address that data base and changes to it**: [25]**

[25: You should, of course, make such changes and additions to this section as are necessary to fit your bank’s situation. However, the following items are important security elements, and it is strongly suggested that if any of them are deleted or materially weakened there be alternative procedures added to this model policy.]

* Access to bank records and systems via publicly available instant messaging (IM) software is prohibited. Firewalls and operating rules are to block IM delivery and file-sharing, as well as other rules management deems advisable to minimize risks arising from IM access. If the bank uses an internal instant messaging system, appropriate controls will be implemented to protect any information that is stored or processed by the system.
* To guard against external intrusion, our most sensitive and vital records and data (to be defined in detail by the TSC) will be maintained, at a minimum, on the bank’s most secure network/intranet or a secure vendor network.
* To the maximum extent practical, we will maintain separate networks segments for internal use, departmental use, connections between branches, Internet access, EDP/Federal Funds, etc.
* All computers or computer systems which are accessible through internal networks or external lines, modems, or similar devices must be protected by employment of measures such as appropriate firewalls and virus detection programs. See the section “Cyber Threats,” below, for additional detail.
* Authorized users may make information-only changes to non-transaction parts of the core system in accordance with written authorizations and procedures. All systems will be designed so that transactional entries, whether to deposit or loan or any other transactional account, can be made only through established EDP procedures. For example (this is not a complete listing): **[26]**

[26: This section should state the specific policy and practices to be followed in your bank. The following two examples illustrate two distinct approaches to this, either of which may be modified to fit your situation, or you may elect an entirely different approach.]

* New account personnel or bank officers may make changes regarding a customer's address or type of accounts used, but not make entries to the customer accounts themselves.
* Loan officers may update or add information to a borrower's credit file, but may not change the terms or amount of an existing loan or make direct entry of a new loan.

### Domain Name [27]

[27: Modify this section to reflect your bank’s Web site(s) and protection methods.]

To protect our online identities and to prevent customer confusion, reputation harm, fraud and legal disputes bank management will employ the following practices:

* Registration and timely renewal of our bank’s domain name(s) to assure that our bank acquires and retains ownership of the Internet addresses that we desire.
* Acquire more than one domain name(s) to retain control over the use of all similar names.
* Ensure that our security considerations regarding our domain name(s) are in place to prevent Internet users from locating information and resources about our customers from the Internet.
* Prevent unauthorized changes to our bank’s domain name information by ensuring that proper controls are in place for authenticating and authorizing all requests for modifications to its registration.
* Assess periodically all security features for customer information.
* Report any suspicious activity involving our bank’s domain name(s) according to the existing instructions for filing Suspicious Activity reports with our primary federal regulator and law enforcement agencies.

## Cyber Threats

Technological advances in computer hardware, software, and communications have promoted greater efficiency and improved service; however, they have also made these infrastructures potentially more vulnerable to disruption or incapacitation by a wide range of physical or computer‑based (cyber) threats.

Our bank recognizes that its vulnerabilities are increasing steadily, and the means to exploit those weaknesses are readily available. The costs associated with an effective attack continue to drop. The basic attack tools of the cyber attacker are a computer, internet access, telephone, and user‑friendly hacker software. Cyber-attacks can take the form of:

* Denial or disruption of computer or telecommunications services.
* Monitoring of computer or telecommunications systems.
* Disclosure of proprietary, private, or classified information stored within or communicated through computer or telecommunications systems.
* Modification or destruction of computer programming codes, computer network databases, stored information, or computer capabilities.
* Manipulation of computer or telecommunications services resulting in fraud, financial loss, or other criminal violations.
* Threats to destroy or disclose data or program files.

To address external attacks and to mitigate their consequences, our bank will:

* Install and maintain a strong intrusion detection system which will:
* Be capable of detecting and recording attempts to break into the bank's computer system.
* Be supported by operating procedures, to be developed by the TSC, for handling such attempts.
* Be resistant to outside attacks.
* Identify and report on deviations from normal processing.
* Be difficult to deceive.
* Be supported by human review of reported activities. Such reviews will be part of the normal operating procedure of the bank. Successful intrusion attempts will often be preceded by unsuccessful attempts that the system should be capable of capturing for analysis.
* Ensure that we have updated, regularly tested incident response and disaster recovery plans to minimize the impact of infrastructure attacks, or infrastructure problems which would be disruptive to our bank's ability to conduct business**. [28]**

[28: This element should be coordinated with, and perhaps implemented by, your bank’s contingency planning and/or emergency preparedness and disaster recovery policies.]

* Maintaining appropriate cyber insurance coverage.
* Additionally, the TSC will review on an ongoing basis existing programs and consider additional procedures which our bank may implement to avoid becoming a cyber-attack victim, including: **[29]**

[29: Some of the following elements will overlap with other parts of this model policy. You may find it useful, however, to retain them in this section in order to call attention to their role in protection against external intrusion.]

* Maintaining adequate expertise, either internally or through the use of third-party providers, to administer, secure, and monitor network security.
* Carefully planning network design and architecture in terms of connectivity, placement of key components, and firewalls. This includes avoiding unnecessary or unused components and services which may unwittingly enable penetration by increasing the potential vulnerabilities.
* Implementing a physical security program that controls and limits the access to computing and information resources to only those who absolutely require such access.
* An authentication system, incorporating logical access controls to computing and information resources that include a program for issuing user IDs, password requirements, anti‑virus programs, and monitoring.
* Using a log‑in banner to ensure that unauthorized users are warned that they may be subject to monitoring.
* Using a real-time intrusion detection system and employing adequate safeguards to ensure the integrity of that detection system itself.
* Reporting significant unauthorized access attempts to the FBI Computer Crimes unit and/or by use of the Suspicious Activity Reporting System.
* Ensuring regular use of virus detection software.
* Review of any newly installed systems or equipment to ensure that its security parameters and settings are consistent with our security risk policies and practices.
* Using software and integrity checkers to identify unauthorized changes to software, and protection of these checkers themselves against changes or compromise.
* Using encryption of data for transmission and storage, commensurate with the levels of risk and the costs involved.
* Maintaining accurate and complete records of users and their activities for analysis, recovery, and development of additional security measures, as well as for possible legal action. Personally identifiable information collected in this manner must be safeguarded and limited in use to conform with applicable privacy laws and regulations.
* Monitoring employee Internet usage and review of policies and guidelines regarding usage.
* Identifying and implementing controls over dial‑in modems that gain access to internal networks.
* Monitoring the environment for unauthorized devices.
* Staying abreast of FS-ISAC and other security advisories.
* Ensuring that audit trails are turned on.
* Making backups of damaged or altered files.
* Maintaining air-gapped backups.
* Encrypting files.
* Encrypting transmissions.
* Using secure firewalls.
* Conducting regular background checks of employees and contractors in sensitive positions.
* Communicating with peers about best practices to protect against identified threats.

## Audit Trails and Detection Measures

Auditing provides an essential control mechanism for detecting deficiencies and managing risks in the implementation of technology. We will ensure that this is accomplished by persons, either internal or external or both, who are qualified to assess the specific risks that arise from specific uses of technology. These specialists will be consulted during the planning process to ensure that technology‑related systems can be audited thoroughly and in a cost‑effective manner.

All sensitive databases and systems will include programs which provide for:

* Audit trails.
* Pre-auditing which defines “auditable events” such as successful and denied file access attempts, file modification, system time/date changes, etc.
* Post-audit procedures, which detect unauthorized users or other threats, by screening of pre-audit data.
* Reporting of actual or attempted unauthorized intrusion or uses of data or systems to the TSO, board of directors, and regulatory and law enforcement agencies by use of Suspicious Activity Reports.

## Intrusion Response Procedures

Intrusion response procedures will be developed, instituted, and regularly tested by the TSO with the advice of the TSC and approval of the board of directors. These procedures will address:

* The priority and sequence of actions to respond to an intrusion, including the containment and elimination of the intrusion and system restoration.
* Gathering and retaining information on the intrusion that enables recovery while facilitating subsequent actions by law enforcement.
* The authority of the TSO and operating and other personnel to act, whether by request or pre-approval, and the process for escalating the intrusion response to progressively higher degrees of intensity and senior management involvement.
* Availability of necessary resources to respond to intrusions.
* System restoration tools and techniques, including the elimination of the intruder’s means of entry and back doors, and the restoration of data and systems to the pre-intrusion state.
* Notification and reporting to operators of other affected systems, users, regulators, incident response organizations, and law enforcement, including the filing of SARs.
* Periodic testing.
* Staff training and requirements.

## Equipment and Software

It is a major objective, within cost effectiveness and risk control constraints, that all equipment and software be standardized and compatible with other equipment and software, existing and planned.

### Personal Computers

Personal computers (PCs), including laptop models, are susceptible to misuse which can result in harm to bank equipment, programs, and data. Therefore, the following special directives, in addition to all other parts of this policy statement, apply to personal computers**: [30]**

[30: This list should be modified to express your bank’s policy in this regard.]

* Bank owned PCs, except for laptop models assigned to or signed out by specific authorized individuals, are not to be taken from bank premises.
* Privately owned PCs are not to be used on bank premises or for bank purposes except during emergency situations with the approval of the TSC.
* Only authorized software is to be used on bank PCs.
* Bank owned PCs are to be used only for banking purposes. For example, entertainment, personal use, or similar software are not to be installed in or used on bank computers.
* Bank owned PCs are to be used only by authorized and trained, or in-training, individuals.

### Software

It is essential that all software used with bank computers or computer systems meet the objectives for compatibility and standardization, and be free of programming flaws or viruses. Therefore, no software (including “freeware” or “shareware”) may be installed on the bank’s computer systems without first being evaluated and approved by the TSO and authorized by the TSC. **[31]**

[31: Alternatively, you may wish to leave this authority at the level of the TSO without requiring TSC authorization.]

## patch Management [32]

[32: This model policy assumes that your bank will include it within an existing policy which establishes lines of authority and responsibility.]

Inadequate patching of software vulnerabilities exposes our bank to significant risk. Software vulnerabilities can cause system unavailability, create security weaknesses, or corrupt critical system components or data. Software vulnerabilities that result in security weaknesses can leave computer systems unprotected and open to access and criminal misuse of bank information by unauthorized parties, such as computer hackers.

Therefore, our bank will initiate and maintain a formal patch management process, meeting the objectives and standards set forth in this policy statement, supplemented by written procedures to the extent deemed appropriate by management.

### Monitoring Software Vulnerabilities and Identifying Patch Information

It is essential that software be monitored for vulnerabilities and identification of patches. Relevant patch information can be identified by subscribing to or reviewing the following sources of patch information, to the extent deemed appropriate by management to our bank:

* Vendor web sites
* Vendor patch alert e-mail list subscriptions
* Third-party security vendor web sites and e-mail alert
* Third-party subscription or periodic vulnerability scanning and reporting services
* Third-party public service security web sites and e-mail alert services
* Internet discussion news groups related to patch management

### Evaluating the Impact of Patches

After a patch has been identified, an impact assessment of the application of the patch will be performed on our information system and business environment, including a technical evaluation, a business impact assessment, and a security evaluation:

* A technical evaluation assessing whether the patch will correct a problem with the services and features of the application that we are using.
* A business impact assessment determining if applying the patch, or not applying the patch, will impact business processes and when may be an appropriate time for patch installation (i.e., immediately, after hours, or over the weekend).
* A security evaluation determining whether there are security implications that were not identified during the technical evaluation. Even though there may be no performance benefit to applying a patch, there may be security benefits. Patches may also be installed on software that may be loaded on a system but is currently inactive.

To the extent that our bank maintains its own internal computer network, but utilizes vendor supplied banking applications, patches will not be installed to our operating system until the banking application vendor has assured us that the operating system patch will not interfere with the banking application software. However, new patches must be evaluated as soon as possible. **[33]**

[33: If this paragraph is not applicable to your bank, it may be omitted from your policy.]

### Testing and Installing Software Patches

Each patch should be tested prior to installation to ensure that it will function as expected and be compatible with other systems. Patches are to be tested at a system level as well as in a quality assurance environment prior to their installation in the production environment. Evaluation and testing should also ensure that the installation of a patch or software update does not open vulnerabilities previously corrected or produce new vulnerabilities. Application of patches in the production environment is subject to normal change management procedures to minimize the risk of disruption due to installation of the patch. Testing should also occur in the production environment after installation.

### Special Reporting Requirements

This patch management program is to be discussed in the annual report to the Board of Directors pursuant to the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 CFR 364, Appendix B, Section III(F).

## Computer Systems

It is our policy and objective, to the extent feasible and cost effective, to establish and maintain a centralized file server to avoid all unnecessary duplications and redundancies, and make that file server available to all bank employees who have an official need for such information**. [34]**

[34: This paragraph should be tailored to your bank's practices and intentions.

"Computer systems," as used in this section, may be in the form of a local area network (LAN) or a wide area network (WAN), or any other form that links together two or more terminals with one or more servers. A terminal may consist of either a PC or a more limited use "dumb terminal."

### Equipment and Software Vendors

The purchase of software and hardware from outside vendors will be subject to the following minimum criteria:

* Appropriate due diligence and ongoing monitoring will be exercised in evaluating the vendor’s reputation, financial status, and viability.
* The hardware or software must be appropriate to the bank system's requirements and specifications.
* Consideration must be given to the impact on existing systems and hardware and compatibility with existing resources.
* The purchase must pass an appropriate cost/benefit analysis.
* Responsibility for hardware and software support and security must be identified and be within the responsible party's capabilities.
* The system must be adequately documented to enable the bank to properly utilize and maintain the software.
* Adequate training must be recognized and provided by either the bank or the vendor, as specified in the purchase agreement. Adequate operating manuals and/or tutorial programs must support hardware and software.

### Independent Servicers

Independent servicers may be utilized to design, maintain, or operate a bank computer system. Any use of an outside servicer will be subject to a comprehensive and adequate written contract and be monitored on an ongoing basis as to:

* Its financial condition, which must provide reasonable assurance that the servicer can continue to meet the bank's needs on an ongoing basis.
* Timely and accurate fulfillment of its responsibilities.
* Adherence to sound internal controls and independent audit coverage, as appropriate to the servicer's engagement, consistent with our policy standards and requirements for in-house services.
* Adequate insurance coverage at the servicer and/or bank level to provide necessary protection to the bank.

## Audit

The bank auditor, or a designated technology specialist counterpart, has the same responsibilities toward the audit of bank computer systems as exist for manual systems. Systems are to be designed to provide adequate audit trails to the extent practicable. Changes made to a database by a user are to be identified as to date and the individual making the change. The views of the auditor will be solicited and considered before changes are made in existing systems or the introduction of new systems.

## Contingency Planning and Protection

All bank computer systems, including hardware and the data contained in them, are subject to and included in the bank's Contingency Planning Policy.

## Security Awareness Program

The TSO, in cooperation with the human resources department, will design, initiate and conduct an ongoing security awareness program for all employees with the objective of giving users a clear understanding of the procedures and controls necessary for a secure environment. The security awareness program should reinforce the bank's security policy and program and may include, for example, instructions regarding password protection, Internet security procedures, user responsibilities, and employee disciplinary actions.

Our bank’s program will, at a minimum:

* Set forth policies, procedures and controls to safeguard the bank's information.
* Define individual responsibilities.
* Describe enforcement and disciplinary actions for non‑compliance.

## Exceptions to Policy [35]

[35: Make changes in this section as necessary to reflect your general requirements for changes to any bank policy.]

Exceptions to this policy may be approved, but only by one of the following two methods. Any such approval must be obtained in advance of the action or practice involved:

* In a manner provided for within this policy; for example, by specific delegation of authority to the TSC.
* By approval of the board of directors.

## Review of Policy

The board of directors shall review this policy at least annually, making such revisions and amendments as it deems appropriate. The Technological Services Committee (TSC) will assist in such reviews and will bring specific matters requiring attention to the board of directors.