2004

Information security program development

William Ward Wells

INFORMATION SECURITY
PROGRAM DEVELOPMENT

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Business Administration

---

by

William Ward Wells

June 2004

INFORMATION SECURITY

PROGRAM DEVELOPMENT

A Project

Presented to the

Faculty of

California State University,

San Bernardino

by

William Ward Wells

June 2004

Approved by:

[redacted] 27 MAY 04

C.E. Tapie Rohm, Jr., Ph.D., Chair, Information & Decision Sciences Date

[redacted]

Mo T. Vaziri, Ph.D., Information & Decision Sciences

[redacted]

Patrick S. McInturff, Ph.D., Department Chair, Management

ABSTRACT

Customer privacy concerns, recent legislation and financial industry regulatory requirements have created the need for financial institutions to create detailed information security plans.

Banking, healthcare and other industries which collect and process private, sensitive data are now required by law to implement information security plans to protect their customer's data from internal and external compromise. More specifically, legislation such as the Gramm-Leach-Bliley Act and the privacy protection sections of the California Civil Code require financial institutions to develop and implement a detailed information security plan, and ensure it remains current with the financial institution's legal and technological environment.

This project reviews Arrowhead Credit Union's Information Security Program structure and contents.

ACKNOWLEDGMENTS

Dr. C.E. T. Rohm, Jr.

Dr. P. McInturff

Dr. M. Vaziri

DEDICATION

To

Jennifer W. and Madison E. Wells

William R., Ph.D and Margaret S. Wells

Winston R. Wells, Ph.D

Richard E. Wells

TABLE OF CONTENTS

CHAPTER FOUR: FINDINGS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

BACKGROUND

Arrowhead Credit Union

Arrowhead Credit Union is a full service, member-owned financial institution serving San Bernardino and Riverside Counties in southern California. Founded in 1949 as San Bernardino County Central Credit Union to serve San Bernardino County employees, the credit union quickly grew and now serves over 200 employer groups. As part of this wider group of customers, the credit union changed its name to Arrowhead Credit Union in 1996 and additionally began serving Riverside County. As a member-owned financial cooperative, the credit union does not have stock-holders or private ownership, and the board of directors serve on a volunteer basis.

Membership in the credit union is available to anyone who lives, works, worships or attends school in San Bernardino and Riverside counties. Upon opening an account, a one-time $5 membership fee is collected to join the credit union. Members have the right to attend annual credit union meetings, and vote to elect the credit union's board of directors.

The board of directors, in concert with the credit union's supervisory committee, oversee the credit union's activities and manage them through the President/Chief Executive Officer. A traditional management structure exists beneath the President/CEO. The credit union employs approximately 660 full time staff and an additional 150 part time employees, making it one of the largest employers in the two county area.

The credit union's assets are currently in excess of $750 million. By asset size, this ranks it in the top 50 credit unions in California, and the top 200 in the nation. The credit union has approximately 140,000 customers (members), with a potential to serve over three million customers.

Arrowhead has 22 branches geographically located throughout San Bernardino and Riverside Counties. The branches are located in areas of population concentrations with the boundaries of Barstow to the north, Hemet to the east, South Corona to the south, and Chino Hills to the west. These branches are a combination of traditional "stand-alone" branches that are located in shopping centers and strip malls, and through a partnership with Stater Bros Markets, a local supermarket chain, seven branches are located inside supermarkets. Members also have a choice of 70 ATMs in San Bernardino and Riverside counties to make fee-free deposits and withdrawals, and an additional 18,000 non-surcharge ATMs nation-wide through the Co-Op ATM Network.

A complete line of financial services are available to credit union members including:

- Savings accounts
- Checking accounts
- Personal lines of credit
- Vehicle loans
- Real Estate loans

As part of the credit union's goal of providing comprehensive financial services to its members, other financial services are available through the credit union's subsidiaries:

- Arrowhead Financial Group, Incorporated
    - Investment Services
    - Financial Planning
    - Tax preparation
    - Insurance Services
- Arrowhead Trust, Incorporated

  - Personal and business trust services
  - IRA planning services
  - Employee benefit plans
- Member Business Services, LLC
  - Commercial lines of credit
  - Money Market accounts
  - Payroll services
  - Business checking services

The credit union is governed by the California Department of Financial Institutions (DFI), and since its deposits are federally insured, also adheres to the National Credit Union Association's (NCUA) guidelines.

Network Overview

Arrowhead Credit Union's network infrastructure is in the format of a basic star or hub and spoke configuration. The credit union has a central data center which contains the credit union's core data processing system, and a distributed Windows 2000 TCP/IP network using to distribute information.

The credit union's 22 branch locations, 13 stand alone ATMs (ATMs not located at a branch or administrative facility), two remote subsidiaries, and six administrative locations are connected via point-to-point T1s and fractional frame relay circuits. Internet connectivity is provided through a local ISP with dual T1 bandwidth. The credit union's extranet connects external vendors also via frame relay circuits. To minimize dependence on one single telephone and data service carrier, three four separate carriers are utilized:

- Verizon
- SBC
- Time Warner Telecommunications
- AT&T

The basic configuration of the credit union's wide area network is shown in the Figure 1:

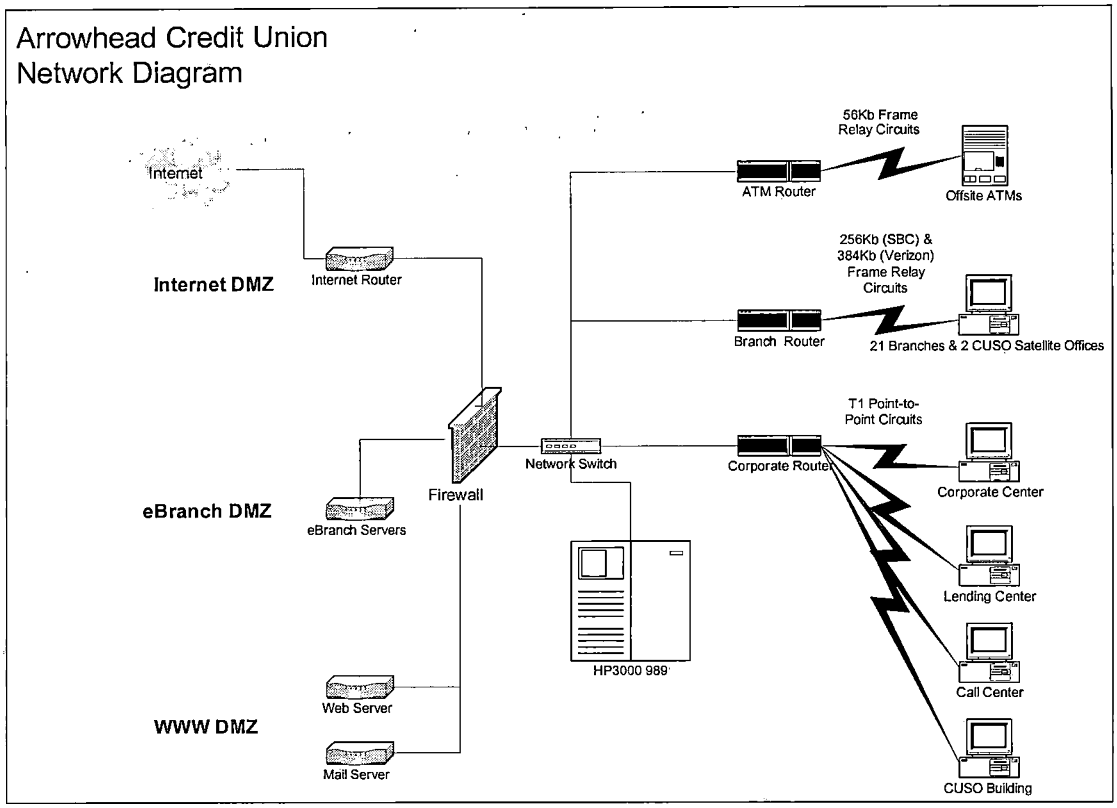


Figure 1. Network Diagram

All external connections are isolated on neutral DMZ networks and managed by the credit union's central firewall. Additional machines protect the internal network by utilizing intrusion detection technologies, spam blocking, and other defenses which monitor and act on malicious traffic attempting to enter the credit union's private network.

The local area networks contain approximately 800 PCs, 65 servers and 150 printers. All hardware is standardized by manufacturer, model and specification.

The Windows 2000 operating system is utilized by all desktop and server machines. Hardware and software setup and "lockdown" procedures are adhered to.

The credit union's systems store sensitive, private data related to members' financial transactions and identity. This data contains information that could be easily exploited if compromised. All external data connectivity is performed over secure private lines, When public Internet systems are utilized, all data is encrypted using 128-bit SSL cryptography. File exchanges with outside entities are performed only on a contract basis, with appropriate non-disclosure agreements in place. Data files are encrypted using PGP and other technologies before transmittal.

Information Systems Department

The Information Systems department at Arrowhead Credit Union is headed by the Senior Vice President/Chief Technology Officer. The Senior Vice President (SVP) reports directly to the Executive Vice President. The Vice President Information Systems reports to the SVP CTO.

The information systems department organization chart is in Figure 2:

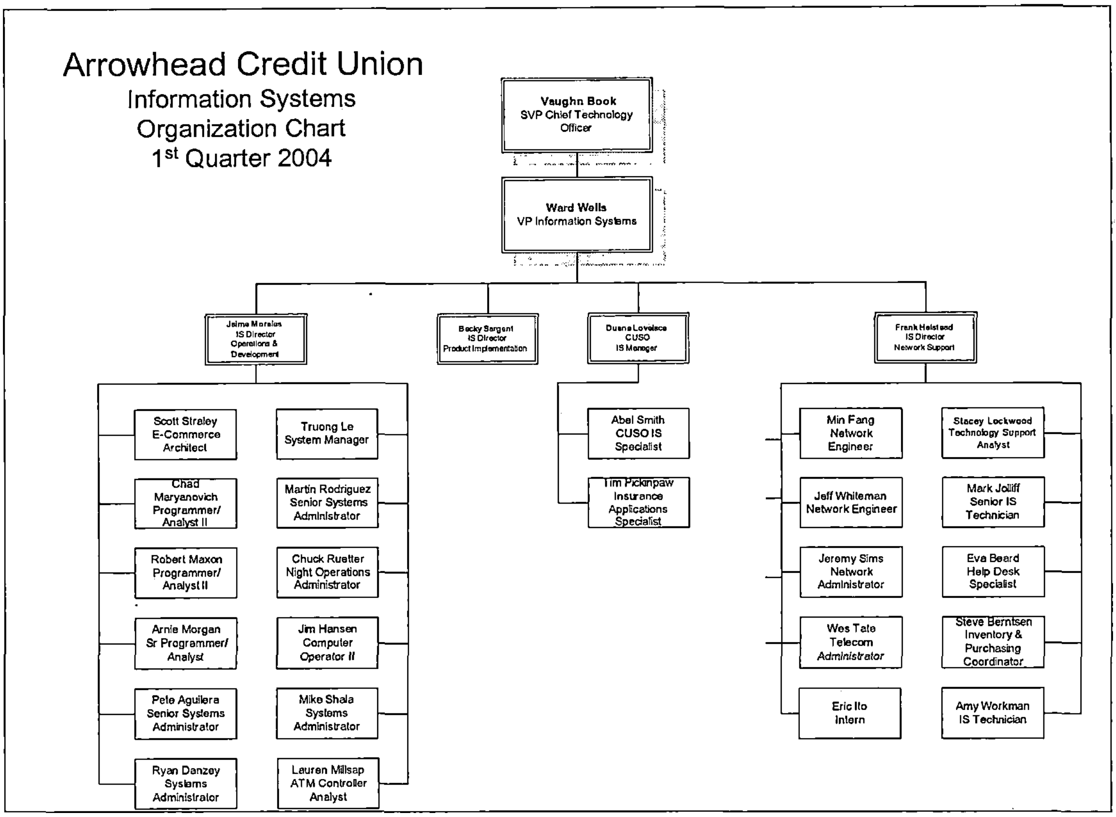


Figure 2. Information Systems Organizational Chart

The Information Systems department has grown considerably over the past five years. It currently consists of 30 full time staff, and is broken down into five major area of concentration:

- Management
  - Senior Vice President/Chief Technology Officer
  - Vice President Information Systems
  - IS Directors and Managers

- Operations and Development
    - Application development
    - E-commerce development
    - Project implementation
    - Core system operations
- Network Support
    - Local and wide area networks
    - Internet connectivity
    - Network security
    - Telecommunications
    - Help Desk support
- Product Implementation
    - Product implementation
    - Quality control
    - System documentation
    - Conversion testing
- Subsidiary Support
    - Hardware and software support
    - Application support
    - Vendor liaison

The major areas of responsibility for each of these groups are shown in Figure 3:

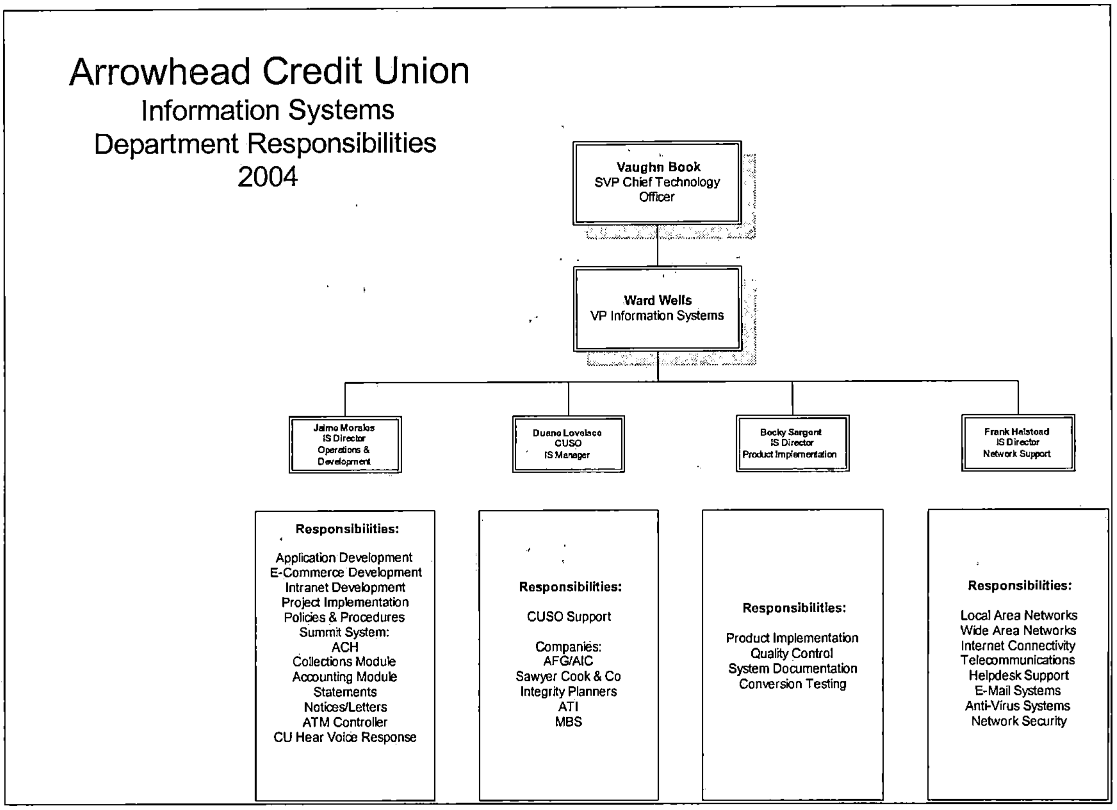


Figure 3. Information Systems Department Responsibilities

With the exception of the help desk staff, all staff are hired with previous experience and a four-year college degree. All staff are required to continue updating the skills and obtain industry certifications. Generous opportunities are afforded to staff to take classes, attend seminars and obtain certification during working hours and at credit union expense.

Staff tenure averages at approximately five years, with average annual turnover of between three and five percent. Eleven staff members have over five years of service with the department, three have over 10 years service. Every effort possible is made to retain employees and ensure their continuing growth.

Privacy Laws

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act was passed by Congress in 2003. Title V of the act specifically addresses privacy issues involved with financial institutions. Section 6801 "Protection of Non-Public Personal Information" requires financial regulatory agencies to ensure that financial institutions have in place safeguards (Federal Trade Commission, 2003)

- to insure the security and confidentiality of customer records and information
- to protect against any anticipated threats or hazards to the security or integrity of such records
- to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

As a federally insured financial institution, Arrowhead Credit Union is subject to regulations of the National Credit Union Association (NCUA). The NCUA issued regulation Part 748 specifically to address requirements of the Gramm-Leach-Bliley Act. A detailed summary of the act's requirements is included in Appendix A.

California Civil Codes

In response to growing public concern, and the federal Gramm-Leach-Bliley Act, California passed Civil Code Section 1798.29 to specifically address companies' obligations in the event of inadvertent disclosure of private customer information. Customers of any agency that owns or licenses computerized data that includes personal information (State of California, 2003) must notify its customers in situations where information systems are breached and/or confidential information is disclosed.

Civil Codes 1798.29, 1798.82, 1798.83 and 1798.84 specifically describe what types of data are deemed confidential, provide timelines and methods for notification, and specific penalties for failing to comply with the codes. The specific language of these civil codes in included in Appendix B.

National Credit Union Association Regulations

The National Credit Union Association (NCUA) is the federal regulatory agency in charge of monitoring the operations of federally insured credit unions. In response to the Gramm-Leach-Bliley Act, the NCUA issued regulation Part 748. The regulation requires credit union's to create and implement an information security plan, and to present such report on demand during annual examinations. (National Credit Union Association, 2001) The specific language of this regulation part is included in Appendix C.

CHAPTER TWO

INFORMATION SECURITY PROGRAM

Introduction

The Gramm-Leach-Bliley Act (GLBA) requires all federal agencies to establish standards relative to administrative, technical and physical safeguards of consumer information. In response, the National Credit Union Administration issued a revision to the NCUA Rules and Regulations Paragraph 748. These rules and regulations require each federally-insured credit union to develop a written security program.

As part of Arrowhead Credit Union's ongoing commitment to ensuring security and protection of our members' privacy the credit union has developed an information security program which meets the requirements laid out by the NCUA.

Arrowhead Credit Union's information security program consists of five major areas:

- Risk Assessment Evaluation
- Information Security Policies
- Network Security Monitoring
- Employee Awareness Training
- Annual Presentation to Board of Directors

Risk Assessment

The key to implementing a successful information security program is identifying and understanding the internal and external threats that could result in the unauthorized disclosure, misuse, alteration or destruction of member information and the systems that manage this information. In 2003 Arrowhead developed a comprehensive methodology to assess the risks to its systems and the data they contain. The methodology was applied to all of the organization's information systems including those related to e-Commerce activities.

The process involved listing each technology and vendor service utilized by the credit union, and categorizing these systems based on the data they process or store. Threats and vulnerabilities were listed for each technology along with any existing controls. The controls were then categorized, and definitions for control adequacy and residual risk were developed, and applied to each technology. Reports were then produced showing vulnerabilities, controls and a risk rating for each technology. These reports are used to determine areas where sufficient and insufficient controls exist.

The overall assessment indicates the credit union is doing very well protecting its information assets. Systems were identified requiring additional attention, and will be carefully examined by Information Systems management.

This methodology will be used on an annual basis to ensure credit union systems maintain their high level of risk aversion and security. In addition, all new technologies will be evaluated and added to the risk management system before implementation.

Policies

As a result of completing the risk assessment process, the credit union has completely reviewed and revised its information security policies. In addition, new policies were added to address up and coming risks as well as new regulatory guidance.

The new and revised policies will be presented to the Board of Directors for their approval in accordance with the credit union's standard procedure approval guidelines.

Monitoring

The credit union contracts for an annual third party, independent verification that the organization's security practices are effective and well managed. In May 2003 Arrowhead engaged Clifton Gunderson LLP to perform an external internet vulnerability assessment. During this assessment, Clifton Gunderson tested for over 400 specific vulnerabilities including:

- Potential threats and vulnerabilities facing external network perimeter
- System configuration policy vulnerabilities
- Denial of service (DOS) vulnerabilities
- Email open relay vulnerabilities and email blacklist

The Clifton Gunderson assessment identified no high risk, no medium risk and 12 low risk vulnerabilities. The report states "Since no high or medium risk vulnerabilities were found, no action needs to be taken. We consider the Low Risk vulnerabilities to be informational, and may not require any corrective action." (Goldenson, R. 2003) The report also stated "The results of our vulnerability assessment detected few addressable weaknesses in the configuration of the entities, as of the date of our testing. While nearly every assessment we perform identifies weaknesses, whether low, medium or high risk, we seldom find so few high and medium risk vulnerabilities. You should be proud of this accomplishment" (Goldenson, R. 2003).

Based on the extensive scope of Arrowhead's technology operations, management has determined that a single, annual 3rd party internet vulnerability assessment is not sufficient to ensure the organization is following current best practices in configuring and managing its system resources. However, due to the cost of such engagements, it is not feasible to have them performed more frequently. To fill this gap, the credit union has chosen several tools which allow it to perform automatic internet vulnerability scans as often as needed.

Qualys Guard is a web based security service allowing the credit union to perform on-demand vulnerability assessments and management. This service identifies security vulnerabilities, provides detailed remediation instructions, tracks which staff have been assigned to fix them and provides feedback on whether or not the problem has been addressed. Qualys updates its vulnerability database on a daily basis and allows the credit union to stay abreast of new security issues and to address those issues before they lead to a system compromise.

Arrowhead also uses the Nessus security scanner to audit both internal and internet connected systems. Nessus is an open source security tool that aims to provide the internet community with a free, powerful, up-to-date and easy to use remote security scanner. The results of Nessus scans are managed by an in-house database that ensures any security or configuration issues it detects are corrected in a timely manner. Follow-up scans are used to ensure any problems have been fixed correctly and do not reoccur.

To ensure that data security remains the highest priority for the staff supporting the organization's information systems, Arrowhead has instituted monthly security meetings. These meetings provide a forum for discussing Arrowhead's security posture, identifying new risks, evaluating new security tools, and ensuring that the organization's policies and procedures are being followed on a consistent basis. The agenda typically includes a review of the latest Qualys and Nessus scans, discussion of new vulnerability alerts, software patches and vendor updates, follow-up on any outstanding security issues and a review of changes to the organization's firewall rule set. This meeting has become an effective tool for keeping staff up-to-date and informed on vital security information.

Employee Education

Arrowhead has also launched an education program to ensure all of the organization's employees know protecting the privacy of member information is their responsibility. All employees were required to attend this training during the program's initial role out and it is presented to all new employees as part of new hire training. The program is also available for employees to review through the intranet.

The program covers many important security topics including:

- The importance of maintaining security to protect member data
- Password security
- E-mail usage and e-mail related security concerns

- Desktop/laptop computer policies
- Secure use of modems
- Internet access
- Threats of the inadvertent disclosure of information over the phone through social engineering
- Employee responsibilities
- General security tips

As part of an ongoing commitment to educating staff on how to keep member information secure, all staff are required to retake this training on an annual basis.

Annual Presentation to Board of Directors

Each fall the credit union's Chief Technology Officer presents an update on the information security plan and the general state of security of the credit union's data assets to the board of directors. This presentation is typically delivered as a Power Point presentation, with supporting documentation given to the directors as required. The presentation consists of updates on the following topics:

- Risk assessment evaluation
- Information security policies

- Network security monitoring
- Employee awareness training

A copy of the current information security plan is securely archived with the presentation material in the formal board meeting minutes, and made available to regulatory agencies only on demand.

CHAPTER THREE

METHODOLOGY

Overview

As part of Arrowhead Credit Union's annual systems security review, and to ensure compliance with privacy provisions of the Gramm-Leach-Bliley Act (GLBA), a risk assessment is performed annually to identify vulnerabilities in electronic systems, and to assess the likelihood and impact of threats, and sufficiency of controls to mitigate risks.

The process involves listing each technology and vendor service utilized by the credit union, and categorizing these systems based on the data they process or store. Threats and vulnerabilities are listed for each technology, and controls are specified for each vulnerability. Controls are then categorized, and definitions for control adequacy and residual risk are developed, and applied to each technology. Reporting is produced showing vulnerabilities, controls and a risk rating for each technology, as well as reports showing areas where sufficient and insufficient controls exist.

This risk assessment is conducted annually by the Senior Vice President/Chief Technology Officer, Vice President Information Systems, and IS Director Operations and Development.

Systems identified as requiring additional attention will be carefully examined by Information Systems management.

The risk assessment will be presented to the credit union's board of directors annually as part of the information security program update. A similar methodology will be used on an annual basis to ensure credit union systems maintain their high level of risk aversion and security.

The credit union's information systems risk assessment process is based on the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook's Information Security Risk Assessment guidelines (Bong, K. 2003):

- Obtain listings of information system assets (e.g., data, software, and hardware). Inventories on a device-by-device basis are helpful in risk assessment as well as risk mitigation. Inventories should consider whether data resides in house or at a service provider.

- Determine threats to those assets, resulting from people with malicious intent, employees and others who accidentally cause damage, and environmental problems that are outside the control of the organization (e.g., natural disasters, failures of interdependent infrastructures such as power and telecommunications facilities).
- Identify organizational vulnerabilities (e.g., ineffective training, inadequate expertise or resource allocation, and inadequate policies, standards, or procedures).
- Identify technical vulnerabilities (e.g., vulnerabilities in hardware and software, configurations of hosts, networks, workstations, and remote access).
- Document current controls and security processes, including both information technology and physical security.

- Identify security requirements and considerations (e.g., GLBA).
- Review and update the risk assessment at least once a year, or more frequently in response to material changes in any of the six actions above.

The information systems risk assessment process is broken down into thirteen major steps:

1. Determine data classification categories
2. Inventory systems
3. Classify inventoried systems
4. Determine initial risk
5. Group technologies
6. List vulnerabilities and threats
7. List controls for each vulnerability and threat
8. Classify controls
9. Determine control adequacy
10. Determine residual risk
11. Generate reports
12. Report results
13. Annual review and update

Step 1: Determine Data Classification Categories

The type of data a system stores, processes, or transmits determines how critical that system is. Developing classification factors for data helps determine which systems put the credit union at a higher risk. Classification factors that rate the importance of security, reliability, and availability of the data are included. Table 1 contains the eight identified data classification categories:

Table 1. Data Classification Categories and Factors

1	Contains non-public personal information about our members as defined in the GLBA privacy regulations.
2	Contains credit union, employee, or member information that should be restricted to a limited number of our employees.
3	Contains credit union, employee, or member information that should be restricted from non-employees.
4	Contains information that is relied upon for risk management or decision making purposes
5	Contains information that could be altered or tampered with for fraudulent purposes
6	Contains information that could be altered or tampered with for financial gain
7	Contains information that is critical to the our internal operations
8	Contains information that is critical to our ability to service our members.

Step 2: Inventory Systems

The second step involves generating a list of all systems in use that store, process, or transmit data. The systems list includes hardware, software, and vendor provided services.

At this stage it is indicated whether the system is a technology or a vendor service. In this context, a technology is a system for which the credit union has control over the security, integrity, or availability. This includes systems managed locally such as server hardware, backup tapes, local databases, and desktop applications. A vendor service is any system for which the vendor has access to the data, or for which the credit union relies on the vendor for integrity or availability. Examples of vendor services include data communication circuits, statement printing vendor, or the credit union's payroll processing service.

Some systems appear as both a technology and a vendor service. For example, a data communication line serving as the credit union's Internet connection is considered a vendor service because the credit union relies on a vendor to keep the circuit secure and available. However, the credit union has some control over the circuit's security by encrypting sensitive member data before transmitting information.

Step 3: Classify Inventoried Systems

Step three involves the determination of which data classification categories (developed in Step 1) are applicable to each technology or vendor service.

It is possible for a technology or vendor service to apply to all, some or none of the data classification categories.

Step 4: Determine Initial Risk

Step four involves the determination of initial risk levels for the identified systems. Risk levels are determined by the impact of events on financial strength and security, non-compliance with regulations, inability to conduct operations, and loss of reputation.

Four categories of initial risk were developed:

Highest Initial Risk. Failure or compromise of this technology or vendor

- Can cause disclosure of private customer information
- Can cause us not to stay in compliance

- Can cause significant impact on the reputation of the company
- Can cause insolvency

High Initial Risk. Failure or compromise of this technology or vendor

- Can prevent us from doing business for an unacceptable period of time.
- Can cause significant impact on the reputation of the company
- Can cause significant financial loss for the company

Medium Initial Risk. Failure or compromise of this technology or vendor

- Can cause degraded service to our customers
- Can delay internal operations for a short period of time
- Can minimally impact reputation
- Can cause a small to medium financial loss for the company

Low Initial Risk. Failure or compromise of this technology or vendor will not cause the conditions indicated above.

Four risk tiers were created by the correlation of the earlier determined data classification factors to the attributes listed above:

Tier 1: Highest Risk.

- Any system containing Category 1 data (GLBA protected member information)

Tier 2: High Risk.

- Any system containing Category 7 data (critical to operations) or Category 8 data (critical to member service).

Tier 3: Medium Risk.

- Any system containing data in Categories 2 through 6

Tier 4: Low Risk.

- Any system that does not fulfill any of the classification categories

Step 5: Group Technologies

To reduce the effort of the risk assessment process by eliminating redundancies, eight technology groups have been created containing systems with similar vulnerabilities.

Grouping technologies provides gains in terms of reducing the effort required to perform the risk assessment, but may also add the potential for error to the system. If necessary, the credit union will "fine tune" the technology groups to make them more specific, thus potentially increasing the accuracy level.

The eight technology groups identified are shown in Table 2:

Table 2. Technology Groups

Technology Groups
Core Systems
Network Infrastructure
File Servers
Internal Applications/Servers
External Applications/Servers
Laptops/Portable Devices
Desktop PCs
Vendors/Service Providers

Step 6: Identify Vulnerabilities and Threats

A list of vulnerabilities and threats has been identified based on indications of how technologies could be compromised. Vulnerabilities included physical threats such as disasters and theft, and virtual vulnerabilities such as viruses due to un-patched operating systems.

Each technology group was then examined to determine which vulnerabilities and threats applied to each group.

Step 7: Identify Controls

After the vulnerabilities or threats potentially impacting credit union systems have been determined, a list of controls in place to aid in mitigating damage or loss is created. The list contains controls currently in place ranging from backup generators to prevent electrical power losses, to desktop anti-virus software used to prevent network virus attacks.

These controls are then compared to the list of vulnerabilities or threats to determine which vulnerabilities or threats they impact.

Step 8: Classify Controls

To adequately control a threat or vulnerability, tools or processes need to be in place to prevent a compromise from occurring, tools or processes in place to detect and alert the credit union if a compromise has occurred, and tools or processes in place to allow the credit union to recover from a compromise quickly and prevent future occurrences.

This step involves the determination of which category (or categories) each control falls into. The following definitions are used:

Preventative Control. A system or technology whose purpose is to prevent an attack attempt or exploit from being successful. A system or technology whose purpose is to prevent a hardware failure from impacting service. Examples of preventative controls include: strong passwords, firewalls, clustered servers, physical access restrictions, and encryption.

Detective Control. A system or technology whose purpose is to detect an attack, compromise, or hardware failure and alert an administrator in an appropriate time frame. Examples of detective controls include: intrusion detection systems, physical security systems, centralized management tools, SNMP, automated log file monitoring, content monitors, virus scanners, and integrity checkers.

Corrective Control. A system or technology that enables the credit union to better respond to and recover from an incident, as well as prevent future occurrences. Corrective controls include incident response programs and systems that record activity, events, or changes for future research.

Policy. The control requires an end user or vendor to follow a policy or contract for it to be effective.

Step 9: Determine Control Adequacy

At this point, definitions are determined for the three levels of control adequacy:

- Strong
- Adequate
- Weak

Different definitions are developed based on the initial risk tier. What is an adequate level of control for medium or low risk systems may not be adequate for higher risk systems.

To determine the definitions, we first considered what constitutes a strong, adequate, or weak level of control, and then applied this to the control categories of preventative, detective, and corrective, to produce definitions by which to calculate the adequacy of the level of control.

Control Adequacy Definitions

Higher Risk Systems (Tier 1 and Tier 2)

Strong

- Assumes layered security, a reliable means for detecting and alerting to a compromise or failure, a means for tracking events and changes or researching past events, and a process to respond, recover, and prevent future occurrences.
- For a given vulnerability, there exists:
  - at least two layers of preventative controls which directly prevent exploit of this vulnerability
  - at least one detective control which will reliably detect an exploit of this vulnerability in a very short time

  - at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences

<u>Adequate</u>

- Assumes there is a control in place preventing every threat or vulnerability from being successful, as well as a means for detecting and responding to compromise or failure.
- For a given vulnerability, there exists:
  - at least two preventative controls which directly prevent exploit of this vulnerability
  - at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences

  OR

  - at least one preventative control which directly prevents exploit of this vulnerability

    - at least one detective control which will reliably detect an exploit of this vulnerability
    - at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences

Weak

Does not meet the criteria above

Medium-Low Risk Systems (Tier 3 and Tier 4)

Strong

- Assumes layered security, a reliable means for detecting and alerting to a compromise or failure, a means for tracking events and changes or researching past events, and a process to respond, recover, and prevent future occurrences.
- For a given vulnerability, there exists:
    - at least two layers of preventative controls which directly prevent exploit of this vulnerability

- at least one detective control which will reliably detect an exploit of this vulnerability
- at least one corrective controls which will improve our ability to respond, recover, and prevent future occurrences

OR

- at least two layers of preventative controls which directly prevent exploit of this vulnerability
- at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences

<u>Adequate</u>

- Assumes there is a control in place preventing every threat or vulnerability from being successful, as well as a means for detecting or responding to and correcting compromise or failure.
- For a given vulnerability, there exists:

- at least one preventative controls which directly prevents exploit of this vulnerability
- at least one detective control which will reliably detect an exploit of this vulnerability
- at least one corrective controls which will improve our ability to respond, recover, and prevent future occurrences

OR

- at least one preventative control which directly prevents exploit of this vulnerability
- at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences

Weak

Does not meet the criteria above.

Step 10: Determine Residual Risk

To determine residual risk definitions are created based on the initial risk tiers and the control adequacy. The residual risk definitions are:

- High residual risk
- Moderate residual risk
- Low residual risk

Using a "weakest link" philosophy, if there is even one weakly controlled vulnerability for a technology, then that technology is determined to have weak controls overall. For a technology to have strong controls overall, every vulnerability must be strongly controlled.

Residual Risk Rating Definitions.

- High Residual Risk
    - Any system of Tier 1 (Highest), Tier 2 (High), or Tier 3 (Medium) Initial Risk with Weak controls to threats and vulnerabilities
- Moderate Residual Risk
    - Any system of Tier 1 (Highest) or Tier 2 (High) Initial Risk with Adequate controls to threats and vulnerabilities
    - Any system of Tier 4 (Low) Initial Risk with Weak controls to threats and vulnerabilities

- Low Residual Risk
    - Any system (Tier 1 through 4) Initial Risk with Strong controls to threats and vulnerabilities
    - Any system of Tier 3 (Medium) or Tier 4 (Low) Initial Risk with Adequate controls to threats and vulnerabilities

The residual risk matrix in Table 3 illustrates the relationship between controls, initial risk and resulting residual risk:

Table 3. Residual Risk Matrix

	Tier 1 (Highest) Initial Risk	Tier 2 (High) Initial Risk	Tier 3 (Medium) Initial Risk	Tier 4 (Low) Initial Risk
Strong Controls	Low Residual Risk	Low Residual Risk	Low Residual Risk	Low Residual Risk
Adequate Controls	Moderate Residual Risk	Moderate Residual Risk	Low Residual Risk	Low Residual Risk
Weak Controls	High Residual Risk	High Residual Risk	High Residual Risk	Moderate Residual Risk

Step 11: Generate Reports

After applying the definitions, reports are created to determine overall control adequacy for each system.

Data Classification Report. Lists system inventory technology/vendor status, technology group, initial risk tier and data classification categories.

System Risk Summary. Lists system inventory, initial risk tier, worst control adequacy, and resulting residual risk level.

System Detail Report. Detailed report of all systems including: initial risk tier, resulting residual risk level, associated vulnerabilities, applicable controls and control adequacy levels.

General Control Adequacy Report. Detailed list of vulnerabilities, associated controls, control type, and control adequacy.

Step 12: Report Results

The Gramm-Leach-Bliley Act requires annual reporting to corporate leadership of

- Status of information security program
- Compliance with Interagency Guidelines
- Risk assessment
- Risk management and control decisions
- Service provider arrangements
- Security violations and management response

- Recommendations for changes to the info security program

The risk analysis will be included in the annual report to the Board of Directors on the credit union's management.

Step 13: Annual Review and Update

The structure of this risk assessment process allows the credit union to build on the previous years' results rather than start over from scratch each year. The extra time saved by not repeating the effort will be used to "fine tune," or make the groups and vulnerabilities more specific to obtain more accurate results.

Where necessary, technologies, vulnerabilities, and controls will be added throughout the year as changes are made within the credit union, and then regenerate the reports to determine how overall risk has been impacted.

CHAPTER FOUR

FINDINGS

The risk assessment process focused on 54 systems identified as being critical to the credit union's operations and containing or processing sensitive member data. The majority (39) of these were in-house systems owned and operated by the credit union, with the balance consisting of a mix of vendor services and systems such as the Fed-Line ACH system. The system breakdown is as follows in Table 4:

Table 4. System Classification Summary

Technology	39
Vendor	11
Both	4
Total Systems	54

Initial Risk Determination

After evaluating the initial risk levels determined for these systems, it was determined that the majority of systems have a "highest level" of initial risk. No critical systems were identified to have a "low level" of initial risk. The initial risk evaluation is shown in Table 5:

Table 5. Initial Risk Level Summary

Initial Risk	
Highest	74%
High	11%
Medium	15%
Low	0%

Data Classification

Each system was classified into the eight applicable categories based on what types of data the system contains, the possibility for use or misuse its data, and the criticality of data to the credit union's operations. Table 6 contains the data classification summary information:

Table 6. Data Classification Summary

Non-Public Information (GLBA)	74%
Information Restricted to Employees	87%
Information Restricted to Non-Employees	85%
Risk Management or Decision Making	31%
Altered for Fraudulent Purposes	87%
Altered for Financial Gain	76%
Critical to Operations	31%
Critical to Member Service	43%

Technology Groups

The 54 identified systems were categorized into eight technology groups. These groups contain systems with similar potential vulnerabilities and threats, and helped streamline the risk assessment process by allowing the focus to be on classes of technologies rather than on individual systems. Table 7 contains the breakdown of technology groups:

Table 7. Technology Group Summary

Core Systems	2%
Network Infrastructure	15%
File Servers	4%
Internal Applications/Servers	48%
External Applications/Servers	6%
Laptops/Portable Devices (PDAs)	2%
Desktop PCs	2%
Vendors/Service Providers	22%

Vulnerabilities and Controls

Common threats and vulnerabilities to were identified and assessed for each technology group. These vulnerabilities dealt with internal and external threats, threats from hardware and software failures, and threats related to breakdowns in the adherence to policies and procedures.

As part of the identification of the credit union's efforts to mitigate the 38 vulnerabilities, 82 controls were identified and related to the applicable vulnerabilities. Only controls whose actual practice was currently in place were related to the identified vulnerabilities.

The vulnerabilities were then rated based on their control's preventative, detective, corrective or policy status producing a control adequacy rating shown in Table 8:

Table 8. Control Adequacy Summary

Control Adequacy	
Strong	76%
Adequate	22%
Weak	2%

These control adequacy ratings were then correlated with the systems identification list to produce the residual risk rating for each system.

Residual Risk Determination

Overall, the risk assessment indicates the credit union's systems are in a very good state of risk control. 94% of all systems received a low or moderate residual risk level. The remaining 6% comprise three systems where opportunities for risk reduction exist.

The System Risk Summary report (see appendix) breaks the credit union's systems into the matrix shown in Table 9:

Table 9. Residual Risk Summary

Resulting Risk Level	Count	% of Total Systems
High Residual Risk	3	6%
Moderate Residual Risk	44	81%
Low Residual Risk	7	13%
Total Systems	54	100%

Systems identified as having high residual risk are:

- E-Branch home banking system
- Exchange e-mail servers
- Internet web server

The following information in Table 10 details the control adequacy summary for all vulnerabilities related to these systems:

Table 10. Control Adequacy Summary

Control Adequacy	
Strong	72%
Adequate	24%
Weak	4%

The primary reason for this high risk level is the previously mentioned "weakest link" method employed to determine residual risk.

A total of 25 vulnerabilities were identified for each of these systems. Each of the three systems identified have 18 vulnerabilities with "strong" control adequacy, six vulnerabilities with "adequate" controls, and only one vulnerability with a "weak" rating. This "weak" rating requires the systems to be rated with high risk despite the existence of 24 other adequate and strong controls in place.

The detailed vulnerability listing for these systems is shown in the Table 11:

Table 11. Vulnerability and Related Control Adequacy Detail

Vulnerability	Control Adequacy
Dormant User Accounts	Strong
Downloading Infected Software	Strong
Hardware Failure of Servers	Strong
Incomplete/Non-Existent Backups	Strong
Infected Software or Files	Strong
Internet Denial of Service Attack	Strong
Malicious Internal Employee	Strong
Password Cracking	Strong
Password Sniffing - Internet	Strong
Physical Theft/Loss	Strong
Power Failure	Strong
Social Engineering	Strong
Telecommunication Outages	Strong
Unpatched Operating Systems	Strong
Vulnerable CGI Programs	Strong
Weak Passwords	Strong
Website Defacement	Strong
Worm or Self-Propagating Virus	Strong
Capture & Decryption of Secure Data	Adequate
IP Spoofing	Adequate
Unnecessary Open Ports	Adequate
Natural Disaster	Adequate
Data Corruption Due To Software Patches	Adequate
Unattended Logged In Terminal	Adequate
DNS/Website Spoofing	Weak

The assessment tool rated the "DNS/Website Spoofing" vulnerability as the only identified vulnerability with inadequate risk aversion controls in place. DNS spoofing refers to the risk of a malicious person or organization hijacking the organization's web site by redirecting its domain name (for example arrowheadcu.org) and redirecting it to another web site. The domain name server used to resolve Arrowhead's domain names is maintained by our internet service provider and thus is not directly under Arrowhead's control. This increases the risk that an improper configuration of this system would not be noticed.

Recommendations

In an effort to reduce the risk level of the three systems identified as having high residual risk, the credit union will research and implement controls to attempt to mitigate the DNS/Website Spoofing vulnerability by the end of the first quarter 2004.

Suggested strategies involve:

- Working with the credit union's Internet service provider to monitor DNS entries and Internet traffic levels to Arrowhead's websites

- Implementing procedures to measure website requests with the aim of identifying any dramatic decrease in traffic
- Subscribing to commercially available 24x7 DNS monitoring services for automated alerts, reporting and general DNS health check information
- Developing internal applications to monitor website content and alert administrators to suspected anomalies

The implementation of a combination of these strategies will allow the credit union to increase its awareness of its DNS/website health, ensure configuration errors are not unintentionally made during installation and setup procedures, and alert staff to suspected spoofing anomalies on a near-real time basis.

Systems identified as having moderate residual risk will also be reviewed by the end of the 2nd quarter 2004 to identify areas where changes may be made to reduce risk.

Systems with a low residual risk level will be continually reviewed to ensure they maintain their security level and improved wherever possible.

As part of the credit union's ongoing risk awareness process, all new systems will be assessed using this methodology before being introduced into the production computing environment. This will allow the credit union to maintain an up-to-date list of systems and information assets, and aid in future annual risk reviews.

Reports

The following detailed reports are included in Appendix D.

Data Classification Report

Lists system inventory technology/vendor status, technology group, initial risk tier and data classification categories.

System Risk Summary

Lists system inventory, initial risk tier, worst control adequacy, and resulting residual risk level.

System Detail Report

Sample detailed report of all systems including: initial risk tier, resulting residual risk level, associated vulnerabilities, applicable controls and control adequacy levels.

General Control Adequacy Report

Detailed list of vulnerabilities, associated controls, control type, and control adequacy.

Policy Review

Arrowhead Credit Union is required by law to protect member data stored and transmitted on its systems. In order to create an environment where this protection is commonplace and rigorously enforced, information security polices have been developed. These polices govern:

- Physical access controls
- Risk assessment requirements
- Software controls
- Employee access
- Data transmission and encryption standards
- Vendor management

Physical Access Controls

Procedures governing physical access controls govern how access is provided to credit union computing devices. Requirements include security concerns such as locked rooms and entry logs, and heating and ventilation requirements.

Risk Assessment Requirements

The credit union's policies require an annual risk assessment be performed on all credit union computing systems. This risk assessment is to cover system inventories, identified vulnerabilities, control adequacy, and follow-up items for remediation efforts.

Software Controls

Software control policies dictate what types of software are allowed to be used on the credit union's PCs and how it is approved and acquired. In a corporate environment, it is essential that all software be compatible, fully licensed and as consistent as possible. It is also crucial that unapproved software not be introduced into the credit union's environment, and that all software additions, modifications, and deletions are managed and orchestrated by the Information Systems department.

Employee Access

Employee access to credit union data must be authorized, managed and tracked. Policies exist to govern which staff positions have access to specific data, and how and when exceptions are made. All exceptions must have a compelling case behind them, and are allowed to be made only at the vice president level and above. Full documentation for each exception must be created and stored.

Password requirements are also covered by credit union policies. These policies govern the length and content of passwords, password complexity, aging and expiration. Detailed password procedures have been developed at the credit union to implement these strict standards.

Data Transmission and Encryption Standards

In order to exchange information with business partners, the credit union must transmit data into and out of its protected systems. In order to ensure these transmissions are secure and not vulnerable to compromise, technologies such as SSL & PGP encryption are utilized. Data is only transmitted to authorized entities, and strict non disclosure agreements exist to ensure further protection of transmitted data.

Vendor Management

Management of the credit union's data processing and information exchange vendors is critical to ensuring the security of the credit union's data. For internal systems, vendors must provide written assurance that their systems are secure, contain no hidden entry points, and maintain compliance with current industry security practices. The security practices of external vendors (such as application service providers) receive strict attention. Detailed annual security reviews, such as the SAS70, are required from each vendor. Vendors are also heavily scrutinized during the pre-implementation due-diligence process to ensure their existing operational standards and safeguards are sufficient.

Individual policies provide high-level direction for management. Detailed procedures have been developed to implement each policy. Procedures provide the day-to-day, specific actions that need to take place to ensure compliance with the policies, and provide reporting tools to archive how compliance with policies is monitored.

The comprehensive text of the credit union's information systems policies is in Appendix E.

Network Security Monitoring

Arrowhead Credit Union recognizes the necessity of having a secure environment for its data, while also needing to balance the need for external connectivity to information and services on the Internet. To accomplish this, the credit union's network is connected to the Internet via multiple high speed data circuits. To protect the internal network for harm, and to ensure the security and integrity of data, the credit union utilizes a firewall, intrusion detection systems, log review procedures and server and router lockdown procedures. The credit union performs internal and external penetration scans to identify vulnerabilities and perform remediation to ensure these network assets are properly configured to only allow appropriate traffic.

External Monitoring

Each year, the credit union contracts with an independent, outside information technology auditing firm to perform network penetration testing. The firm examines the credit union's external Internet presence. Testing is performed from the firm's test center, outside the Arrowhead Credit Union network by conducting non-disruptive tests that will not disturb the credit union's computer and communications services. If there is a possibility of a disruption, the auditing firm works with the credit union to schedule the testing and notify any departments that might be affected. All security tests are performed from outside the firewall to create a true picture of the credit union's external Internet presence.

The purpose of the assessment is to assist in identifying vulnerabilities and to implement safeguards within the credit union's enterprise security architecture. The auditing firm utilizes tools such as the Internet Scanner from Internet Security Systems (ISS), Windows NT/2000 test scripts, and other automated utilities as needed. The review classifies the vulnerabilities as high, medium, or low, and also provides an explanation of the risks involved with each exposure. Internet Scanner is recommended as the computing and security industry's preferred solution for network vulnerability assessment and audit analysis. This security scanning tool directly addresses the single most important aspect of organizational network risk management: identifying and addressing technical vulnerabilities. Internet Scanner also provides detailed technical policies and performs scheduled and selective vulnerability probes and assessments of the network's communication services, operating systems, key applications, and routers. Intrusion detection software searches for those vulnerabilities used by unscrupulous attackers to probe, investigate, and attack the credit union's network. Its powerful reporting and analysis engines analyzes the credit union's vulnerability conditions and provide a series of corrective action, trend analysis, audit variance, and configuration reports (Goldenson, 2003).

In addition, the auditing firm provides recommendations and detailed instructions to help implement countermeasures. The recommendations assist in identifying:

- Potential threats and vulnerabilities facing external network perimeter
- Potential threats and vulnerabilities facing internal network infrastructure
- System configuration policy vulnerabilities
- Denial of services vulnerabilities

The penetration testing vulnerability analysis is required to integrate industry best practices and technical expertise. At the test's conclusion, the auditing firm provides the results of the test to the credit union's senior management. It is also common for the auditing firm to, at the request of credit union management, conduct a high level executive briefing to inform management of the testing findings and recommendations.

Internal Monitoring

In addition to the annual external penetration testing, the credit union's Information Systems staff continually monitors the internal network for vulnerabilities. The majority of these vulnerabilities are related to software or operating systems' deficiencies (such as Microsoft Windows 2000), or result from the improper configuration of other aspects of the credit union's system. The credit union's systems need to be continuously monitored to ensure changes or additions to the network do not expose new vulnerabilities.

The information systems staff utilize five primary software packages to monitor the credit union's network:

- Qualys Guard
- Nessus
- Superscan
- Languard
- Entercept

Additionally, software and operating systems on the credit union's network routers and firewall are configured to block intrusions and suspected irregularities from the Internet. These systems look for characteristics of known attacks and are updated when new attacks are discovered.

Qualys Guard. Qualys is a leading intrusion detection and network security company. The company has been credited by Microsoft for finding recent potential vulnerabilities in the Windows operating system, and others. Qualys Guard is a subscription based service, in which the credit union schedules external penetration testing scans to be run from the Qualys network operations center. These scans attempt to do the same penetration testing as the annual external vendor audit, but are run on demand by credit union information systems staff.

The credit union selects which range of IP addresses are to be scanned, and detailed results reports are available usually within one hour of the scan. The reports detail which hosts were found, any information that was gleaned from them (OS version, system name, IP address), and any vulnerabilities that are found. The information systems department's management meets on a bi-weekly basis with the network administration group to review the test results and take whatever appropriate action necessary.

Nessus. Nessus is an open source tool used in the information systems network administration community to externally and internally scan networks for vulnerabilities. Nessus performs similar penetration tests to the external vendor penetration test, and the tests run by Qualys Guard.

Since Nessus is a linux-based tool, the credit union is able to run the software on an externally connected PC (via separate DSL connection) at the credit union, and run an unlimited amount of scans on any type of host. A separate Nessus server is utilized to scan internal networks, including all firewall DMZs.

The Nessus tool provides a detailed assessment of the scanned network hosts. These reports identify what information was found from the hosts (similar to the Qualys reports), and also suggests possible ways to correct any possible vulnerabilities found. Nessus reports are also reviewed by information systems management on a bi-weekly basis.

Superscan. Superscan is a shareware Windows port scanning tool from Foundstone, Inc. The software runs internally on several information systems PCs, and is used to identify vulnerabilities that may exist due to trojans, spy ware and other malicious software that attempts to do harm by opening up different TCP and UDP ports on infected machines. The tool is also useful in identifying deficiencies and irregularities in server and desktop operating system configuration and lockdown methods.

LAN Guard. LAN Guard software is available from GFI, Inc. GFI produces network and message scanning tools for the Microsoft Windows platform. LAN Guard provides network security log monitoring and assists in patch level maintenance efforts. This software is also run in-house and is regularly used to monitor the credit union's Microsoft Windows server and desktop platforms.

Entercept. McAfee Entercept is a host intrusion detection tool from Computer Associates. The Entercept software runs on web-exposed hosts (typically web and mail servers), and performs the tasks of a traditional host-based intrusion detection system such as traffic monitoring, packet examination and warning and blocking activities where warranted.

All information from the various Entercept hosts is collected and compiled in the Entercept monitor application. This application is monitored regularly by network administration staff, and summary information is produced for the credit union's monthly network security meeting.

Employee Information Security Education

In addition to policies, risk assessment, network monitoring efforts, a critical piece of Arrowhead Credit Union's information security plan involves employee training. Employees must be made aware of the importance of information security, potential ways information can be compromised, and their responsibilities for helping keep data secure.

Each year, all employees review a brief Power Point presentation titled "Information Security Training." This presentation covers the overall importance of information security and how it interacts with staff's daily activities at the credit union.

Presentation Overview

- Member data is our most critical asset. This data has been given to us by our members and must be treated with the utmost respect and confidentiality.
- The credit union relies on all staff to keep members' data safe. Each employee has a responsibility to act in a manner that protects information from being compromised, and is obligated to report any incidents if they suspect a compromise has occurred. Employees are also encouraged to make suggestions pertaining to ways information security can be enhanced.
- Credit union systems are only as safe as employees make them. Policies, risk assessment, audits and network monitoring efforts can all be made worthless by an employee inadvertently or intentionally disclosing confidential member information.
- Arrowhead Credit Union views information security very seriously. The credit union is

required by law to have an information security program in place, and is regularly audited to determine its effectiveness.

- Legal action against the credit union can occur if member data is compromised. Steep fines can be levied against the credit union if member data is disclosed. Severe damage to the credit union's reputation can also occur.

Password Security

- Password privacy is essential. Passwords must not be written down or exchanged in e-mail or any other form.
- Password composition must be complex (a mix capitalized letters, numbers, special symbols are required). Common words or names are not to be used.
- Passwords must be changed at regular intervals. Credit union systems require uses to change their passwords on a pre-determined interval. Themes and sequential passwords should never be used.

E-Mail Security

- E-Mail from unknown senders should not be opened. If it is unintentionally opened, attachments to these messages should never be opened. Employees should contact the Information Systems department immediately if they suspect they have opened a virus-infected e-mail or attachment
- Member information should never be communicated through Internet e-mail. Names, account information and balances should not be sent. Placing this information in an Internet e-mail is similar to writing the information down on a postcard and mailing it using the United States Postal Service.
- Arrowhead Credit Union e-mail addresses should only be disclosed for work related purposes. Disclosure for other purposes often exposes staff to spam and other unwanted e-mail. This information could also be used to misrepresent the credit union for fraudulent purposes.

Desktop Computers

- Staff should always sign off the credit union's core data processing system when they complete their work.
- All PCs should be logged off or turned off when unattended. Use of the ctrl-alt-del function is stressed to lock or log off workstations. Automated workstation locking policies are scheduled to activate after predetermined periods of inactivity.
- Unauthorized hardware or software is never to be installed on any credit union computer. Approval from the Information Systems department is required before any additional hardware or software is installed or removed.
- Anti-virus protection software is never to be tampered with or disabled. This is a key part of the computer's ability to protect itself and our data from compromise.
- Documents, spreadsheets and other files are not to be brought into the credit union from home or other computers that lack anti-virus

protection. Anti-virus protection is commercially available at a reasonable price and is not difficult to install and maintain.

Laptop Computers

- Documents containing member information should be password protected. This is one way to attempt to protect the documents in case the laptop is stolen or otherwise compromised.
- "Save Password" boxes on dial-up connections and other places should never be checked. This could allow an unauthorized person access to the credit union's network assets without knowledge of a user's password.
- Laptops should always be turned off and safely stored when not in use. Since the laptop has the propensity to be in areas more vulnerable and public than desktop computers, this is often overlooked. Additionally, it is a good practice to secure laptops that are left in the office overnight.
- Credit union laptops are to be used for work purposes only, unless approved in advance by

the Information Systems department. Additional software should never be installed on a credit union laptop without prior approval.

- Lost or stolen laptops must be reported to the Information Systems department immediately. A stolen laptop represents an intrusion risk to the credit union's network and all access must be immediately terminated.

Modems

- Modems should always be turned off when not in use. Modems should also not be left in the "auto answer" mode. This represents a potential entry point for intrusion into the credit union's network.
- Remote access software such as PC Anywhere or VNC should never be left running unattended. The software is approved for use for specific applications, but should only be turned on when needed, monitored during use, and turned off after work is complete.
- Credit union modem numbers should be closely guarded and only given out where necessary.

- Modems are for work-related purposes only. They should not be used for access to outside services that are not specifically approved by the Information Systems department.

Internet Access

- Internet access is provided as a tool to help improve productivity and enhance member service. Internet access is to be used only for work-related purposes unless otherwise specifically approved. All Internet access is logged and reviewed.
- Programs, screen savers, plug-ins and other files are not to be downloaded or installed on credit union computers. These often represent a security risk, and may interfere with legitimate programs.
- Arrowhead Credit Union information should be disclosed only where necessary. Staff should be conservative in their disclosures, and only provide the minimum information necessary when working on the Internet.

- Remote access program such as "GoToMyPC" are not allowed to be installed on credit union computers. The Information Systems department blocks access into and out of the network to prevent remote PCs from being used, or credit union PCs being controlled remotely.

Phones

- Member information is never to be disclosed to unauthorized persons. Credit union procedures for validating and authenticating members' identities must be followed at all times.
- Credit union computers, software, network information or Internet access are not to be discussed with outside entities. It is very important that we do not inadvertently disclose information that may assist in a future attack or penetration attempt into the credit union's protected computer network.
- Staff should never dial phone numbers or transfer calls from someone claiming to be from the telephone company. This is a common fraud scheme where criminals attempt to gain access

to long distance lines at the credit union's expense. If such a request is made, immediately transfer the call to the Information Systems department.

The Microsoft Power Point slide presentation given to all credit union employees via the corporate intranet is included in Appendix F.

CHAPTER FIVE

CONCLUSION

Information security planning is a critical part of any organization's operations if that organization stores, maintains and is responsible for ensuring the privacy of confidential data. Federal, state and other agencies have provided guidance and requirements for these types of plans to be in place, with specific penalties applicable to non-compliance.

The information security plan for any organization is a living document, and is meant to be continually revisited, revised and updated as the organization's operating, technology and regulatory environments change. These security plans must be supported from the highest levels of any organization.

Information security planning education for both technical and non-technical management and staff is essential. This training should be technical enough to provide necessary information, but relative and meaningful enough to reach the general computer user audience.

Arrowhead Credit Union is committed to protecting its members and their data from the ever changing security threats created by doing business in an increasingly interconnected world. To meet this challenge, the organization has implemented a comprehensive security program. This program involves identifying potential risks, mitigating those risks through policies, procedures and security systems, educating staff on their roll in maintaining the privacy of member information as well as internal and external monitoring of Arrowhead's security posture.

Arrowhead will continue to refine and enhance its information security program as new threats emerge, to stay abreast of industry best practices, and to insure regulatory compliance with new laws, rules and regulations.

APPENDIX A

GRAMM-LEACH-BLILEY ACT

Gramm-Leach-Bliley Act

TITLE V -- PRIVACY

- Requires clear disclosure by all financial institutions of their privacy policy regarding the sharing of non-public personal information with both affiliates and third parties.

- Requires a notice to consumers and an opportunity to "opt-out" of sharing of non-public personal information with nonaffiliated third parties subject to certain limited exceptions.

- Addresses a potential imbalance between the treatment of large financial services conglomerates and small banks by including an exception, subject to strict controls, for joint marketing arrangements between financial institutions.

- Clarifies that the disclosure of a financial institution's privacy policy is required to take place at the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship.

- Provides for a separate rather than joint rulemaking to carry out the purposes of the subtitle; the relevant agencies are directed, however, to consult and coordinate with one another for purposes of assuring to the maximum extent possible that the regulations that each prescribes are consistent and comparable with those prescribed by the other agencies.

- Allows the functional regulators sufficient flexibility to prescribe necessary exceptions and clarifications to the prohibitions and requirements of section 502.

- Clarifies that the remedies described in section 505 are the exclusive remedies for violations of the subtitle.

- Clarifies that nothing in this title is intended to modify, limit, or supersede the operation of the Fair Credit Reporting Act.

- Extends the time period for completion of a study on financial institutions' information-sharing practices from 6 to 18 months from date of enactment.

- Requires that rules for the disclosure of institutions' privacy policies must be issued by regulators within 6 months of the date of enactment. The rules will become effective 6 months after they are required to be prescribed unless the regulators specify a later date.

- Assigns authority for enforcing the subtitle's provisions to the Federal Trade Commission and the Federal banking agencies, the National Credit Union Administration, the Securities and Exchange Commission, according to their respective jurisdictions, and provides for enforcement of the subtitle by the States.

Title V - Sec. 6801. Protection of nonpublic personal information

(a) Privacy obligation policy

It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) Financial institutions safeguards

In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards -

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 6803, 6805 of this title.

NOTE: Pub. L. 106-102, title V, Sec. 510, Nov. 12, 1999, 113 Stat. 1445, provided that: "This subtitle (subtitle A (Sec. 501-510) of title V of Pub. L. 106-102, enacting this subchapter and amending section 1681s of this title) shall take effect 6 months after the date on which rules are required to be prescribed under section 504(a)(3) (15 U.S.C. 6804(a)(3)), except -

(1) to the extent that a later date is specified in the rules prescribed under section 504; and

(2) that sections 504 (15 U.S.C. 6804) and 506 (enacting section 6806 of this title and amending section 1681s of this title) shall be effective upon enactment (Nov. 12, 1999).

APPENDIX B

CALIFORNIA CIVIL CODES

California Civil Code

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.
(2) Driver's license number or California Identification Card number.
(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.
(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.
(C) Notification to major statewide media. (h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.
(2) Driver's license number or California Identification Card number.
(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.
(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.
(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.83. Any waiver of the provisions of this title is contrary to public policy, and is void and unenforceable.

1798.84. (a) Any customer injured by a violation of this title may institute a civil action to recover damages.

(b) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

APPENDIX C

NATIONAL CREDIT UNION ASSOCIATION REGULATIONS

NATIONAL CREDIT UNION ASSOCIATION REGULATIONS

Part 748
REPORT OF CRIME OR CATASTROPHIC ACT PART 748
November 2001
Security Program, Report of
Crime and Catastrophic Act and
Bank Secrecy Act Compliance
§ 748.0–§ 748.2

§ 748.0 Security program.

(a) Each federally-insured credit union will develop a written security program within 90 days of the effective date of insurance.

(b) The security program will be designed to:

(1) Protect each credit union office from robberies, burglaries, larcenies, and embezzlement;

(2) Ensure the security and confidentiality of member records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;

(3) Assist in the identification of persons who commit or attempt such actions and crimes; and

(4) Prevent destruction of vital records, as defined in 12 CFR part 749.

§ 748.1 Filing of reports.

(a) *Compliance Report.* Each federally-insured credit union shall file with the regional director an annual statement certifying its compliance with the requirements of this Part. The statement shall be dated and signed by the president or other managing officer of the credit union. The statement is contained on the Report of Officials which is submitted annually by federally-insured credit unions after the election of officials. In the case of federally-insured state-chartered credit unions, this statement can be mailed to the regional director via the state supervisory authority, if desired. In any event, a copy of the statement shall always be sent to the appropriate state supervisory authority.

(b) *Catastrophic Act Report.* Each federally-insured credit union will notify the regional director within 5 business days of any catastrophic act that occurs at its office(s). A catastrophic act is any natural disaster such as a flood, tornado, earthquake, etc., or major fire or other disaster resulting in some physical destruction or damage to the credit union. Within a reasonable time after a catastrophic act occurs, the credit union shall ensure that a record of the incident is prepared and filed at its main office. In the preparation of such record, the credit union should include information sufficient to indicate the office where the catastrophic act occurred; when it took place; the amount of the loss, if any; whether any operational or mechanical deficiency(ies) might have contributed to the catastrophic act; and what has been done or is planned to be done to correct the deficiency(ies).

(c) *Suspicious Activity Report.* (1) Each federally-insured credit union will report any crime or suspected crime that occurs at its office(s), utilizing NCUA Form 2362, Suspicious Activity Report (SAR), within thirty calendar days after discovery. Each federally-insured credit union must follow the instructions and reporting requirements accompanying the SAR. Copies of the SAR may be obtained from the appropriate NCUA Regional Office.

(2) Each federally-insured credit union shall maintain a copy of any SAR that it files and the original of all attachments to the report for a period of five years from the date of the report, unless the credit union is informed in writing by the National Credit Union Administration that the materials may be discarded sooner.

(3) Failure to file a SAR in accordance with the instructions accompanying the report may subject the federally-insured credit union, its officers, directors, agents or other institution affiliated parties to the assessment of civil money penalties or other administrative actions.

(4) Filing of Suspicious Activity Reports will ensure that law enforcement agencies and NCUA are promptly notified of actual or suspected crimes. Information contained on SARs will be entered into an interagency database and will assist the federal government in taking appropriate action.

§ 748.2 Bank Secrecy Act compliance programs and procedures.

(a) *Purpose.* This Section is issued to ensure that all federally-insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance with the requirements of Subchapter II of Chapter 53 of Title 31, United States Code, the Financial Record keeping and Reporting of Currency and Foreign Transactions Act, and the implementing regulations promulgated there under by the Department of Treasury, 31 C.F.R. Part 103.

(b) *Compliance Procedures.* On or before August 1, 1987, each federally-insured credit union shall develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with record keeping and reporting requirements set forth in Subchapter II of Chapter 53 of title 31, United States Code, the Financial Record keeping and Reporting of Currency and Foreign Transactions Act and the implementing regulations promulgated there under by the Department of Treasury, 31 C.F.R. Part 103. This program shall be reduced to writing, approved by the board of directors of the institution, and noted in the minutes.

(c) *Contents of Compliance Program.* Such compliance program shall at a minimum—

(1) Provide for a system of internal controls to assure ongoing compliance;

(2) Provide for independent testing for compliance to be conducted by credit union personnel or outside parties;

(3) Designate an individual responsible for coordinating and monitoring day-to-day compliance;

and

(4) Provide training for appropriate personnel.

APPENDIX D

RISK ASSESSMENT REPORTS

Data Classification Report

					Cat							
System	Group	Technology	Vendor	Tier (Risk)	1	2	3	4	5	6	7	8
Windows 2000 Servers	File Server	X		Highest	X	X	X	X	X	X	X	X
ADP Payroll System	Vendor/Service	X	X	Highest	X	X	X		X	X	X	
AFS Item Processing System	Internal App/Server	X		Highest	X	X	X	X	X	X	X	X
Avaya & Mitel PBXs	Network Infrastructure	X		Medium		X	X		X	X		
BDI Statement Printing Vendor	Vendor/Service		X	Highest	X	X	X		X	X		X
Call Accounting Server	Internal App/Server	X		Medium		X	X					
CastleRock SNMPc Server	Internal App/Server	X		High							X	
Clarke American Check Ordering	Vendor/Service		X	Highest	X	X	X		X	X		X
Contour RE Processing Software	Internal App/Server	X		Highest	X	X	X	X	X	X	X	X
Co-Op/E-Funds ATM Network	Vendor/Service		X	Highest	X	X	X		X	X		X
COWWW Receipt Archiving Server	Internal App/Server	X		Highest	X	X	X		X		X	
Credit Reporting Modem Server	Internal App/Server	X		Highest	X	X	X	X	X	X	X	X
CUNA Model Management Software	Internal App/Server	X		Medium		X	X	X	X	X		
De La Rue Teller Cash Dispensers	Internal App/Server	X		Medium			X		X	X		
Desktop PCs	Desktop PC	X		Highest	X	X			X	X		
Dynamic Loan Center Server	Internal App/Server	X		Highest	X	X	X	X	X	X	X	X
E-Branch Home Banking System	External App/Server	X		Highest	X	X	X		X	X		
E-Funds Router	Network Infrastructure	X		Highest	X	X	X		X	X		X
Exchange Mail Servers	External App/Server	X		Highest	X	X	X	X	X	X	X	X
Fed-Line Backup Server	Internal App/Server	X	X	Highest	X	X	X		X	X		
Gasper ATM Monitoring System	Internal App/Server	X		High						X	X	
HSM Encryption Key Controller	Internal App/Server	X		Highest	X	X	X		X	X		X
Instant Issue Debit Card Server	Internal App/Server	X		Highest	X	X	X		X	X		
Internet Firewall	Network Infrastructure	X		Highest	X	X	X		X	X		
Internet Mail Server	Internal App/Server	X		Medium		X	X					
Internet Router	Network Infrastructure	X		Highest	X	X	X		X	X		
Internet Web Server	External App/Server	X		Highest	X	X	X		X			
Intranet Database Server	Internal App/Server	X		Highest	X	X	X	X				
Intranet Web Server	Internal App/Server	X		Highest	X	X	X	X				
IPS Sendero Accounting Software	Internal App/Server	X		Medium		X	X	X	X	X		
LAN Switches	Network Infrastructure	X		Highest	X	X	X		X	X		
Laptops/PDAs	Laptop/Portable	X		Highest	X	X			X	X		
MAS 200 Accounting Software	Internal App/Server	X		Medium		X	X	X	X	X		

									Cat			
System	Group	Technology	Vendor	Tier (Risk)	1	2	3	4	5	6	7	8
MaxAttach Storage Servers	File Server	X		Highest	X	X	X	X	X	X		
Maxxar Call-24 Audio Response Units	Internal App/Server	X		Highest	X	X	X		X	X		
Mitel Voice Mail Server	Internal App/Server	X		Medium		X	X		X	X		
Mortgagebot Real Estate Origination	Vendor/Service		X	Highest	X	X	X	X	X	X		
NAVCO Security Monitoring System	Internal App/Server	X	X	Highest	X	X	X	X	X	X	X	
Politzer & Haney ACH Software	Internal App/Server	X	X	Highest	X	X	X		X	X		X
Postilion ATM Controller	Internal App/Server	X		Highest	X	X	X		X	X		X
PSCU Router/Processing PC	Network Infrastructure	X		Highest	X	X	X		X	X		X
PSCU/FDR Debit Card System	Vendor/Service		X	Highest	X	X	X		X	X		X
Qualifile Fraud Detection System	Vendor/Service		X	Highest	X	X	X	X	X	X		
Remote Access Modem Server	Network Infrastructure	X		Highest	X	X	X		X	X		
Salesforce.com CRM System	Vendor/Service		X	Highest	X	X	X		X	X		
SBC Voice & Data Circuits	Vendor/Service		X	High					X		X	X
Sprint Voice Circuits	Vendor/Service		X	High					X		X	X
Summit System	Core System	X		Highest	X	X	X	X	X	X	X	X
Synergy Archiving/Imaging System	Internal App/Server	X		Highest	X	X	X	X	X	X		
Time Warner Voice & Data Circuits	Vendor/Service		X	High					X		X	X
Trial Balance Software	Internal App/Server	X		Highest	X	X	X					
TWS ATM Balancing System	Internal App/Server	X		Highest	X	X	X		X	X		X
Verizon Voice & Data Circuits	Vendor/Service		X	High					X		X	X
WAN Routers	Network Infrastructure	X		Highest	X	X	X		X	X	X	X

System Risk Summary

System Name	Tier Name	Worst Control Adequacy	Resulting Residual
Windows 2000 Servers	Highest Initial Risk	2-Adequate	Moderate Residual Risk
ADP Payroll System	Highest Initial Risk	2-Adequate	Moderate Residual Risk
AFS Item Processing System	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Avaya & Mitel PBXs	Medium Initial Risk	1-Strong	Low Residual Risk
Call Accounting Server	Medium Initial Risk	1-Strong	Low Residual Risk
CastleRock SNMPc Server	High Initial Risk	2-Adequate	Moderate Residual Risk
Contour RE Processing Software	Highest Initial Risk	2-Adequate	Moderate Residual Risk
COWWW Receipt Archiving Server	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Credit Reporting Modem Server	Highest Initial Risk	2-Adequate	Moderate Residual Risk
CUNA Model Management Software	Medium Initial Risk	1-Strong	Low Residual Risk
De La Rue Teller Cash Dispensers	Medium Initial Risk	1-Strong	Low Residual Risk
Desktop PCs	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Dynamic Loan Center Server	Highest Initial Risk	2-Adequate	Moderate Residual Risk
E-Branch Home Banking System	Highest Initial Risk	3-Weak	High Residual Risk
E-Funds Router	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Exchange Mail Servers	Highest Initial Risk	3-Weak	High Residual Risk
Fed-Line Backup Server	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Gasper ATM Monitoring System	High Initial Risk	2-Adequate	Moderate Residual Risk
HSM Encryption Key Controller	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Instant Issue Debit Card Server	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Internet Firewall	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Internet Mail Server	Medium Initial Risk	1-Strong	Low Residual Risk
Internet Router	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Internet Web Server	Highest Initial Risk	3-Weak	High Residual Risk
Intranet Database Server	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Intranet Web Server	Highest Initial Risk	2-Adequate	Moderate Residual Risk
IPS Sendero Accounting Software	Medium Initial Risk	1-Strong	Low Residual Risk
LAN Switches	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Laptops/PDAs	Highest Initial Risk	2-Adequate	Moderate Residual Risk
MAS 200 Accounting Software	Medium Initial Risk	1-Strong	Low Residual Risk
MaxAttach Storage Servers	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Maxxar Call-24 Audio Response Units	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Mitel Voice Mail Server	Medium Initial Risk	1-Strong	Low Residual Risk

System Name	Tier Name	Worst Control Adequacy	Resulting Residual
NAVCO Security Monitoring System	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Politzer & Haney ACH Software	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Postilion ATM Controller	Highest Initial Risk	2-Adequate	Moderate Residual Risk
PSCU Router/Processing PC	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Remote Access Modem Server	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Summit System	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Synergy Archiving/Imaging System	Highest Initial Risk	2-Adequate	Moderate Residual Risk
Trial Balance Software	Highest Initial Risk	2-Adequate	Moderate Residual Risk
TWS ATM Balancing System	Highest Initial Risk	2-Adequate	Moderate Residual Risk
WAN Routers	Highest Initial Risk	2-Adequate	Moderate Residual Risk

System Detail Report

System: Windows 2000 Servers Tier: 1 Highest Initial Residual Risk: Moderate

Classification Categories:
1. Non-public personal customer information
2. Data should be restricted to certain employees
3. Data should be restricted from non-employees
4. Data is relied upon for risk management
5. Data could be altered or tampered with for fraudulent purposes
6. Data could be altered or tampered with for financial gain
7. Data is critical to our internal operations
8. Data is critical to customer service

Vulnerability	Controls	Control Adequacy		
Dormant user accounts	Account and user rights management (Preventative)	Preventative:	3	1-Strong
	Logfile monitoring (Corrective)	Detective:	1	
	Periodic forced password changes (Preventative)			
	Terminated employee process (Preventative)	Corrective:	2	
	User account monitoring (Detective Corrective)			
Downloading infected software from Internet	Desktop antivirus (Detective Corrective)	Preventative:	6	1-Strong
	Desktop software installation policy (Preventative)	Detective:	3	
	Internet use policy (Preventative)			
	Account and user rights management (Preventative)	Corrective:	3	
	Server antivirus (Preventative Detective Corrective)			
	Service pack/security patch tracking system (Detective Corrective)			
	Security patch application (Preventative)			
	User training (Preventative)			
Email viruses	Email antivirus (Preventative Detective Corrective)	Preventative:	5	1-Strong
	Incident response processes (Corrective)	Detective:	4	
	Intrusion detection system (Detective)			
	Awareness and appropriate configuration (Preventative)	Corrective:	4	
	Desktop antivirus (Detective Corrective)			
	Internet use policy (Preventative)			
	Server antivirus (Preventative Detective Corrective)			
	Account and user rights management (Preventative)			

Hardware failure of servers	Hardware redundancy (Preventative)	Preventative:	2	1-Strong
	CastleRock SNMPc monitoring	Detective:	1	
	Backup systems (Corrective)			
	Incident response processes (Corrective)	Corrective:	3	
	Hardware Maintenance Contracts (Corrective)			
	UPS (Preventative)			
Incomplete/non existent backups	Backup monitoring (Detective Corrective)	Preventative:	2	1-Strong
	Backup policies and procedures (Preventative)	Detective:	1	
	Off-site storage contract (Preventative Corrective)			
	Corrective:	2		
Infected software or disks on servers	Server antivirus (Preventative Detective Corrective)	Preventative:	2	1-Strong
	Backup systems (Corrective)	Detective:	2	
	Locked/logged out servers (Preventative)			
	Desktop antivirus (Detective Corrective)	Corrective:	3	
Malicious internal employee	Backup systems (Corrective)	Preventative:	7	1-Strong
	Incident response processes (Corrective)	Detective:	1	
	Locked/logged out servers (Preventative)			
	Authentication event logging (Corrective)	Corrective:	4	
	Account and user rights management (Preventative)			
	Backup policies and procedures (Preventative)			
	Change default passwords (Preventative)			
	Strong passwords (Preventative)			
	User account monitoring (Detective Corrective)			
	Disable or re-name default user accounts (Preventative)			
	Terminated employee process (Preventative)			
Password cracking	Strong passwords (Preventative)	Preventative:	3	1-Strong
	Incident response processes (Corrective)	Detective:	1	
	Enhanced user account and authentication log monitoring (Detective)			
	Account lockout policy (Preventative)	Corrective:	2	
	Change default passwords (Preventative)			

Physical theft/loss	CastleRock SNMPc monitoring	Preventative:	2	1-Strong
	Business resumption plan (Corrective)	Detective:	1	
	Physical access controls (Preventative)			
	Terminated employee process (Preventative)	Corrective:	2	
	Incident response processes (Corrective)			
Power failure	Backup generator (Preventative)	Preventative:	3	1-Strong
	Business resumption plan (Corrective)	Detective:	1	
	CastleRock SNMPc monitoring			
	UPS (Preventative)	Corrective:	2	
	User training (Preventative)			
	Incident response processes (Corrective)			
Social engineering	Locked/logged out servers (Preventative)	Preventative:	3	1-Strong
	Incident response processes (Corrective)	Detective:	1	
	User training (Preventative)			
	Physical access controls (Preventative)	Corrective:	2	
	User account monitoring (Detective Corrective)			
Telecom outages	Incident response processes (Corrective)	Preventative:	2	1-Strong
	CastleRock SNMPc monitoring	Detective:	1	
	ISDN backup (Corrective)			
	UPS (Preventative)	Corrective:	2	
	Multiple telecommunication vendors (Preventative)			
Unpatched operating systems and software - servers	Change management (Preventative Corrective)	Preventative:	4	1-Strong
	Security patch application (Preventative)	Detective:	1	
	Service pack/security patch tracking system (Detective Corrective)			
	User training (Preventative)	Corrective:	3	
	Policies to install only necessary services (Preventative)			
	Incident response processes (Corrective)			

Weak passwords/password guessing	Strong passwords (Preventative)	Preventative:	6	1-Strong
	User account authentication log monitoring (Detective)	Detective:	2	
	Incident response processes (Corrective)			
	Account lockout policy (Preventative)	Corrective:	3	
	Change default passwords (Preventative)			
	Disable or re-name default user accounts (Preventative)			
	Periodic forced password changes (Preventative)			
	User account monitoring (Detective Corrective)			
	User training (Preventative)			
Worm or other self-propagating virus	Intrusion detection system (Detective)	Preventative:	3	1-Strong
	Server antivirus (Preventative Detective Corrective)	Detective:	5	
	Service pack/security patch tracking system (Detective Corrective)			
	Security patch application (Preventative)	Corrective:	4	
	Desktop antivirus (Detective Corrective)			
	Firewall (Preventative Detective Corrective)			
Capture and decryption of secured data transmissions	128 bit encryption Internet comm. (Preventative)	Preventative:	7	2-Adequate
	Firewall (Preventative Detective Corrective)	Detective:	2	
	SSL with signed certificates for secure web services (Preventative)			
	Switched network (Preventative)	Corrective:	1	
	Security controls (Authentication and encryption) placed on			
	Wireless not used in production (Preventative)			
	Physical access controls (Preventative)			
Listening services/open ports on internal systems	Awareness / appropriate configuration (Preventative)	Preventative:	6	2-Adequate
	Security patch application (Preventative)	Detective:	3	
	Incident response processes (Corrective)			
	Policies to install only necessary services (Preventative)	Corrective:	1	
	Vulnerability scanning (Preventative Detective)			
	HTTP Request Filtering (URL Scan) (Preventative Detective)			
	Independent Internet Penetration Testing (Preventative Detective)			

Natural disaster	Backup generator (Preventative)	Preventative:	7	2-Adequate
	Backup policies and procedures (Preventative)	Detective:	0	
	Backup systems (Corrective)			
	Off-site storage (Preventative)	Corrective:	5	
	Off-site storage contract (Preventative Corrective)			
	Incident response processes (Corrective)			
	Fire suppression (Corrective)			
	Disaster recovery contract (Preventative)			
	Risk/Testing/Migration/Recovery plans (Preventative)			
	Business resumption plan (Corrective)			
	UPS (Preventative)			
Password sniffing - private network	Incident response processes (Corrective)	Preventative:	2	2-Adequate
	Intrusion detection system (Detective)	Detective:	1	
	Switched network (Preventative)			
	Periodic forced password changes (Preventative)	Corrective:	1	
Physical access to un-secured logged in terminal	Physical access controls (Preventative)	Preventative:	3	2-Adequate
	Account and user rights management (Preventative)	Detective:	1	
	User account monitoring (Detective Corrective)			
	Account lockout policy (Preventative)	Corrective:	1	
Unprotected shares and trust relationships	Awareness/appropriate configuration (Preventative)	Preventative:	2	2-Adequate
	Intrusion detection system (Detective)	Detective:	1	
	Incident response processes (Corrective)			
	Account and user rights management (Preventative)	Corrective:	1	

General Control Adequacy

Vulnerability	Controls			Control Adequacy
Dormant user accounts	Account and user rights management (Preventative)	*Preventative:*	3	1-Strong
	Logfile monitoring (Corrective)	*Detective:*	1	
	Periodic forced password changes (Preventative)			
	Terminated employee process (Preventative)	*Corrective:*	2	
	User account monitoring (Detective Corrective)			
Downloading infected software from Internet	Desktop antivirus (Detective Corrective)	*Preventative:*	6	1-Strong
	Desktop software installation policy (Preventative)	*Detective:*	3	
	Internet use policy (Preventative)			
	Account and user rights management (Preventative)	*Corrective:*	3	
	Server antivirus (Preventative Detective Corrective)			
	Service pack/security patch tracking system (Detective Corrective)			
	Security patch application (Preventative)			
	User training (Preventative)			
Email viruses	Email antivirus (Preventative Detective Corrective)	*Preventative:*	5	1-Strong
	Incident response processes (Corrective)	*Detective:*	4	
	Intrusion detection system (Detective)			
	Awareness and appropriate configuration (Preventative)	*Corrective:*	4	
	Desktop antivirus (Detective Corrective)			
	Internet use policy (Preventative)			
	Server antivirus (Preventative Detective Corrective)			
	Account and user rights management (Preventative)			
Hardware failure of network devices	Redundant systems (Preventative)	*Preventative:*	3	1-Strong
	Incident response processes (Corrective)	*Detective:*		
	CastleRock SNMPc monitoring			
	Hardware redundancy (Preventative)	*Corrective:*		
	Hardware Maintenance Contracts (Corrective)			
	UPS (Preventative)			

Hardware failure of servers	Hardware redundancy (Preventative)	*Preventative:*	2	1-Strong
	CastleRock SNMPc monitoring	*Detective:*	1	
	Backup systems (Corrective)			
	Incident response processes (Corrective)	*Corrective:*	3	
	Hardware Maintenance Contracts (Corrective)			
	UPS (Preventative)			
Incomplete/non existent backups	Backup monitoring (Detective Corrective)	*Preventative:*	2	1-Strong
	Backup policies and procedures (Preventative)	*Detective:*	1	
	Off-site storage contract (Preventative Corrective)	*Corrective:*	2	
Infected software or disks on desktops	Server antivirus (Preventative Detective Corrective)	*Preventative:*	2	1-Strong
	Backup systems (Corrective)	*Detective:*	2	
	Locked/logged out servers (Preventative)			
	Desktop antivirus (Detective Corrective)	*Corrective:*	3	
Infected software or disks on servers	Server antivirus (Preventative Detective Corrective)	*Preventative:*	2	1-Strong
	Backup systems (Corrective)	*Detective:*	2	
	Locked/logged out servers (Preventative)			
	Desktop antivirus (Detective Corrective)	*Corrective:*	3	
Infected software or disks on web servers	Server antivirus (Preventative Detective Corrective)	*Preventative:*	2	1-Strong
	Backup systems (Corrective)	*Detective:*	1	
	Locked/logged out servers (Preventative)	*Corrective:*	2	
Internet denial of service attack	Internet T1 Provider (Preventative)	*Preventative:*	3	1-Strong
	Incident response processes (Corrective)	*Detective:*	2	
	Border router access control lists (Preventative)			
	Firewall (Preventative Detective Corrective)	*Corrective:*	2	
	Intrusion detection system (Detective)			
Malicious contractor/vendor	Backup systems (Corrective)	*Preventative:*	5	1-Strong
	Incident response processes (Corrective)	*Detective:*	1	
	Locked/logged out servers (Preventative)			
	Authentication event logging (Corrective)	*Corrective:*	4	
	Account and user rights management (Preventative)			
	Physical access controls (Preventative)			
	User account monitoring (Detective Corrective)			
	Change default passwords (Preventative)			
	Disable or re-name default user accounts (Preventative)			

Malicious internal employee	Backup systems (Corrective)	*Preventative:*	7	1-Strong
	Incident response processes (Corrective)	*Detective:*	1	
	Locked/logged out servers (Preventative)			
	Authentication event logging (Corrective)	*Corrective:*	4	
	Account and user rights management (Preventative)			
	Backup policies and procedures (Preventative)			
	Change default passwords (Preventative)			
	Strong passwords (Preventative)			
	User account monitoring (Detective Corrective)			
	Disable or re-name default user accounts (Preventative)			
	Terminated employee process (Preventative)			
Password cracking	Strong passwords (Preventative)	*Preventative:*	3	1-Strong
	Incident response processes (Corrective)	*Detective:*	1	
	Enhanced user account and authentication			
	log monitoring (Detective)			
	Account lockout policy (Preventative)	*Corrective:*	2	
	Change default passwords (Preventative)			
Password sniffing - Internet	128 bit encryption Internet communications (Preventative)	*Preventative:*	3	1-Strong
	Incident response processes (Corrective)	*Detective:*	1	
	Border router access control lists (Preventative)			
	Enhanced user account / authentication			
	log monitoring (Detective	*Corrective:*	2	
	Periodic forced password changes (Preventative)			
Physical theft/loss	CastleRock SNMPc monitoring	*Preventative:*	2	1-Strong
	Business resumption plan (Corrective)	*Detective:*	1	
	Physical access controls (Preventative)			
	Terminated employee process (Preventative)	*Corrective:*	2	
	Incident response processes (Corrective)			
Power failure	Backup generator (Preventative)	*Preventative:*	3	1-Strong
	Business resumption plan (Corrective)	*Detective:*	1	
	CastleRock SNMPc monitoring			
	UPS (Preventative)	*Corrective:*	2	
	User training (Preventative)			
	Incident response processes (Corrective)			

Social engineering	Locked/logged out servers (Preventative)	*Preventative:*	3	1-Strong
	Incident response processes (Corrective)	*Detective:*	1	
	User training (Preventative)			
	Physical access controls (Preventative)	*Corrective:*	2	
	User account monitoring (Detective Corrective)			
Telecom outages	Incident response processes (Corrective)	*Preventative:*	2	1-Strong
	CastleRock SNMPc monitoring	*Detective:*	1	
	ISDN backup (Corrective)			
	UPS (Preventative)	*Corrective:*	2	
	Multiple telecommunication vendors (Preventative)			
Unpatched operating systems and software - clients	Security patch tracking system (Detective Corrective)	*Preventative:*	3	1-Strong
	Security patch application (Preventative)	*Detective:*	2	
	Policies to install only necessary services (Preventative)			
	User training (Preventative)	*Corrective:*	2	
	Users alert via help desk (Detective)			
	Incident response processes (Corrective)			
Unpatched operating systems and software - network devices	Incident response processes (Corrective)	*Preventative:*	4	1-Strong
	Policies to install only necessary services (Preventative)	*Detective:*	1	
	Security patch application (Preventative)			
	Security patch tracking system (Detective Corrective)	*Corrective:*	3	
	User training (Preventative)			
	Change management process (Preventative Corrective)			
Unpatched operating systems and software - servers	Change management process (Preventative Corrective)	*Preventative:*	4	1-Strong
	Security patch application (Preventative)	*Detective:*	1	
	Service pack/security patch tracking system (Detective Corrective)			
	User training (Preventative)	*Corrective:*	3	
	Policies to install only necessary services (Preventative)			
	Incident response processes (Corrective)			

Vulnerable CGI programs	Security patch application (Preventative)	*Preventative:*	6	1-Strong
	Service pack/security patch tracking system (Detective Corrective)	*Detective:*	4	
	Firewall (Preventative Detective Corrective)			
	Intrusion detection system (Detective)	*Corrective:*	3	
	Vulnerability scanning (Preventative Detective)			
	Logfile monitoring (Corrective)			
	Security considered when developing programs (Preventative)			
	Account and user rights management (Preventative)			
	Awareness and appropriate configuration (Preventative)			
Weak passwords/password guessing	Strong passwords (Preventative)	*Preventative:*	6	1-Strong
	Enhanced user account and authentication log monitoring (Detective	*Detective:*	2	
	Incident response processes (Corrective)			
	Account lockout policy (Preventative)	*Corrective:*	3	
	Change default passwords (Preventative)			
	Disable or re-name default user accounts (Preventative)			
	Periodic forced password changes (Preventative)			
	User account monitoring (Detective Corrective)			
	User training (Preventative)			

Website defacement of Internet servers	Vulnerability scanning (Preventative Detective)	*Preventative:*	12	1-Strong
	Firewall (Preventative Detective Corrective)	*Detective:*	4	
	Account and user rights management (Preventative)			
	Awareness and appropriate configuration (Preventative)	*Corrective:*	5	
	Account lockout policy (Preventative)			
	Authentication event logging (Corrective)			
	Backup policies and procedures (Preventative)			
	Backup systems (Corrective)			
	Incident response processes (Corrective)			
	Intrusion detection system (Detective)			
	Security considered when developing programs (Preventative)			
	Security patch application (Preventative)			
	Server antivirus (Preventative Detective Corrective)			
	Strong passwords (Preventative)			
	Web server application not running as admin (Preventative)			
	Web server NTFS permissions (Preventative)			
Worm or other self-propagating virus	Intrusion detection system (Detective)	*Preventative:*	3	1-Strong
	Server antivirus (Preventative Detective Corrective)	*Detective:*	5	
	Service pack/security patch tracking system (Detective Corrective)			
	Security patch application (Preventative)	*Corrective:*	4	
	Desktop antivirus (Detective Corrective)			
	Firewall (Preventative Detective Corrective)			
Capture and decryption of secured data transmissions	128 bit encryption Internet communications (Preventative)	*Preventative:*	7	2-Adequate
	Firewall (Preventative Detective Corrective)	*Detective:*	2	
	SSL with signed certificates for secure web services (Preventative)			
	Switched network (Preventative)	*Corrective:*	1	
	Security controls (Authentication and encryption) placed on			
	Wireless not used in production (Preventative)			
	Physical access controls (Preventative)			

Hardware failure of clients	User training (Preventative)	*Preventative:*	3	2-Adequate
	Hardware Maintenance Contracts (Corrective)	*Detective:*	0	
	Standardized Client Hardware (Preventative)			
	Awareness and appropriate configuration (Preventative)	*Corrective:*	2	
	Incident response processes (Corrective)			
IP spoofing	Firewall (Preventative Detective Corrective)	*Preventative:*	1	2-Adequate
	Incident response processes (Corrective)	*Detective:*		
	Intrusion detection system (Detective)	*Corrective:*	2	
Listening services/open ports on internal systems	Awareness and appropriate configuration (Preventative)	*Preventative:*	6	2-Adequate
	Security patch application (Preventative)	*Detective:*	3	
	Incident response processes (Corrective)			
	Policies to install only necessary services (Preventative)	*Corrective:*	1	
	Vulnerability scanning (Preventative Detective)			
	HTTP Request Filtering (URL Scan) (Preventative Detective)			
	Independent Internet Penetration Testing (Preventative Detective)			
Listening services/open ports on web servers	Awareness and appropriate configuration (Preventative)	*Preventative:*	4	2-Adequate
	Policies to install only necessary services (Preventative)	*Detective:*	1	
	Incident response processes (Corrective)			
	Security patch application (Preventative)	*Corrective:*	1	
	Vulnerability scanning (Preventative Detective)			
Natural disaster	Backup generator (Preventative)	*Preventative:*	7	2-Adequate
	Backup policies and procedures (Preventative)	*Detective:*	0	
	Backup systems (Corrective)			
	Off-site storage (Preventative)	*Corrective:*	5	
	Off-site storage contract (Preventative Corrective)			
	Incident response processes (Corrective)			
	Fire suppression (Corrective)			
	Disaster recovery contract (Preventative)			
	Risk/Testing/Migration/Recovery plans (Preventative)			
	Business resumption plan (Corrective)			
	UPS (Preventative)			

OS/Software installation and patches corrupting data	Backup systems (Corrective)	*Preventative:*	4	2-Adequate
	Change management process (Preventative Corrective)	*Detective:*	0	
	Test lab (Preventative)			
	Backup policies and procedures (Preventative)	*Corrective:*	2	
	Security patch application (Preventative)			
Password sniffing - private network	Incident response processes (Corrective)	*Preventative:*	2	2-Adequate
	Intrusion detection system (Detective)	*Detective:*	1	
	Switched network (Preventative)			
	Periodic forced password changes (Preventative)	*Corrective:*	1	
Physical access to un-secured logged in terminal	Physical access controls (Preventative)	*Preventative:*	3	2-Adequate
	Account and user rights management (Preventative)	*Detective:*	1	
	User account monitoring (Detective Corrective)			
	Account lockout policy (Preventative)	*Corrective:*	1	
Unprotected shares and trust relationships	Awareness and appropriate configuration (Preventative)	*Preventative:*	2	2-Adequate
	Intrusion detection system (Detective)	*Detective:*	1	
	Incident response processes (Corrective)			
	Account and user rights management (Preventative)	*Corrective:*	1	
Vendor inadequate internal controls	Ongoing vendor review (SAS70) (Detective Corrective)	*Preventative:*	1	2-Adequate
	Technology acquisition due diligence (Preventative Detective)	*Detective:*	2	
		Corrective:	1	
Wireless access compromise	Wireless not used in production (Preventative)	*Preventative:*	3	2-Adequate
	Encryption required on WAP (Preventative)	*Detective:*	1	
	Policies against end users setting up WAPs (Preventative)			
	Security monitoring (Detective)	*Corrective:*	1	
	Incident response processes (Corrective)			
	DNS/Website spoofing	*Preventative:*	0	3-Weak
		Detective:	0	
		Corrective:	0	

APPENDIX E

INFORMATION SYSTEMS POLICIES

Information Systems Policies

Policy 10.33 Information Security Policy Statement

IT IS THE POLICY OF THIS CREDIT UNION THAT:
Arrowhead Credit Union shall protect the confidentiality, security, and integrity of each member's nonpublic personal information in accordance with existing state and federal laws.

The credit union will maintain physical, electronic, and procedural safeguards that comply with federal standards to guard members' nonpublic personal information.

The credit union will not gather, collect, or maintain any information about its members that is not necessary in order to offer its products and services, to complete member transactions or for other relevant business purposes.

Management of Arrowhead Credit union shall be responsible for developing, implementing, and maintaining an effective information security program to:

- Insure the security and confidentiality of member records and information.
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any member.

Management shall regularly (no less than annually) report to the board on the current status of the credit union's information security program.

ASSESSMENT OF RISK
In order to assess the risks that may threaten the security, confidentiality, or integrity of member information or member information systems, the credit union shall:

- Identify all reasonably foreseeable internal as well as external threats that can result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems.
- Determine the likelihood as well as potential damage of the internal and external threats.
- Determine the sufficiency of the credit union's policies, procedures and member information systems to control the identified risks.

MANAGEMENT AND CONTROL OF RISK
In order to manage and control the risks that have been identified, the credit union shall:

- Establish written procedures designed to implement, maintain and enforce the credit union's information security program.

- Limit access to the credit union's member information systems to authorized employees only
- Establish controls to prevent employees from providing member information to unauthorized individuals.
- Limit access at the credit unions physical locations containing member information, such as buildings, computer facilities, and records storage facilities to authorized individuals only.
- Provide encryption of electronic member information including but not limited to information in transit or in storage on networks or systems to which unauthorized individuals may have access.
- Ensure that member information system modifications are consistent with the credit union's information security program.
- Implement dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to member information.
- Monitor the credit union's systems and procedures to detect actual and attempted attacks on or intrusions into the member information systems.
- Establish response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies.
- Implement measures to protect against destruction, loss, or damage of member information due to environmental hazards, such as fire and water damage or technical failures.
- Regularly test, monitor, evaluate, and adjust as appropriate, the information security program in light of any relevant changes in technology, and internal or external threats to the credit union's information security systems.
- Regularly test the key controls, systems, and procedures of the information security program.
- Ensure that all contracts with service providers contain appropriate provisions requiring the service providers to protect the confidentiality of the credit union member's nonpublic personal information.

EMPLOYEE TRAINING

Employees should be trained with regard to their responsibilities under this policy. In addition, employees should be trained to recognize, respond to, and where appropriate, report any unauthorized or fraudulent attempts to obtain member information.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.34 Overview of Policies

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Purpose

The purpose of the Information Systems Security policy is to establish minimum-security requirements and controls for the protection of information and association information technology resources. Information security measures at Arrowhead are intended to:

- Protect valuable information assets
- Preserve the privacy of Members and staff
- Reduce the risk of unauthorized access, corruption, destruction, delay or misuse of information assets and critical operations
- Protect the legal position of Arrowhead

Scope

Arrowhead's Information Security Policies apply to information throughout its lifecycle, including creation, distribution, storage and disposal.

These policies are to protect information in all environments in which member information resides, including information that resides with outside parties such as third party providers, which is subject to the same controls used to protect information processed internally.

Adherence to this policy is required by all staff, temporaries, interns, contractors, service providers, and agents who use, have access to, or are responsible for information assets, and those who design, operate, or are responsible for the computer and manual systems which contain the organization's assets.

Resources included in the scope of this security policy statement include, but are not limited to: information (data) in any medium or form including, but not limited to: paper, digital, video, and audio representations; computing hardware and software systems which access and manipulate information; and network systems which transport information. Legal constraints directly affect the use of some of these resources. Credit Union policy may also affect the use of information resources. The multiplicity of needs involving information uses, locations, and protection dictates that a broad spectrum of possible security procedures is necessary. Security risks must be evaluated, and appropriate procedures must be selected and implemented by the individuals responsible for such assets.

Principles
Arrowhead's values, beliefs or philosophies are indicated in our Core Values and mission statement and those values are inherent in, and form the foundation of, the Information Systems Security Policy and the organization's overall security architecture. Arrowhead is dedicated to "Helping members build wealth."

Information Assets
Information assets are data and propriety information in electronic, printed or other forms. They are considered sensitive or critical to Arrowhead's business objectives. All information and data that resides or is transferred on Arrowhead computers or networks, as well as all storage media is property of Arrowhead.

Information Protection and Privacy.
Information assets will be protected at a level commensurate to their value and potential risk to Arrowhead. Protection will ensure the confidentiality, integrity, and availability of Arrowhead's information assets.

All Arrowhead Credit Union users (employees, consultants, contractors and temporaries) must be provided with sufficient training and supporting reference materials to allow them to properly protect and otherwise manage Arrowhead Credit Union information assets. Training materials should communicate that information security is an important part of Arrowhead Credit Union's business, and must be viewed like other on-going business functions such as accounting and marketing. Training and documentation with respect to information security is the responsibility of the Information Systems and Training Departments.

Non-Business Use of Information and Equipment
Arrowhead Credit Union information (product specifications, databases, mailing lists, internal software, computer documentation, etc.) must only be used for the business purposes specifically allowed by management. Use of these information resources for any other reason will be permitted only after an SVP CTO or the Vice President of Information Systems has granted written permission.

Accountability
Users and custodians of Arrowhead's information assets are responsible for the appropriate use, protection and privacy of Arrowhead's information assets. All Arrowhead systems will generate and maintain appropriate audit trails to enable identification of users, critical events and processes.

Availability
Information assets must be available to ensure continued operation of Arrowhead's business objectives. Appropriate measures must be in place to ensure the timely recovery of all information and access by authorized individuals.

Integrity

Information assets must be adequately protected to ensure completeness and accuracy. Validation measures will be utilized to allow detection of inappropriately modified, deleted or corrupted information.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.35 Roles and Responsibilities

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Management

Critical business decisions by our Board of Directors and management team is wholly dependent on the integrity of information and information systems. Arrowhead Credit Union's future competitive advantage will in part be achieved through the appropriate management of information and information systems. Management refers to those staff responsible for directing the activities of other staff.

Management *Responsibilities:*

- Accept accountability for all information assets under their control.
- Authorize user access to information assets as appropriate.
- Ensure compliance with the organization's requirements for information protection by establishing controls that meet or exceed Arrowhead's Information Security Policies.
- Assign and track ownership of responsibility for information assets.
- Provide sufficient resources to protect Arrowhead's information assets.
- Respond appropriately to information security related exposures and losses.
- Know the nature of information used for decision-making (accuracy, timeliness, relevance, completeness, confidentiality, criticality, etc.).
- Ensure that assigned personnel fulfill responsibilities as data stewards, custodians and/or users.

Data Stewards

Data stewards are responsible for making overall control and access decisions for entrusted information assets. The data steward should be the person in the best position to know the organization's business and the value of the information assets. For example, Information Systems Management and department vice presidents can be considered data stewards.

Responsibilities:

- Assign value and classify information.
- Ensure and validate the quality and integrity of information.
- Authorize overall access to information and authorize exceptions.
- Define roles and responsibilities for custody of information.
- Specify protective measures to custodian and users of the information.
- Determine retention and privacy information.

Information Custodian

Custodians have authorized control and physical custody of entrusted information, and provide proper protection in an operational environment. For example, data processing system administrators can be considered Information Custodians.

Responsibilities:

- Comply with organizational and Data Steward specified protection requirements.
- Provide security tools and mechanisms, and physical and procedural safeguards to protect the information from accidental or intentional, but unauthorized disclosure, modification, or destruction.
- Arrange for backup of vital records and their retention in secure locations.
- Inform Data Stewards of potential and real security exposures and weaknesses.

Users

Users are individuals with management-authorized access to information and/or information systems. While scope of access may differ from system to system, all staff are considered Users of information.

Responsibilities:

- Use information only for authorized business purposes.
- Comply with organizational and Data Steward specified protection requirements including Arrowhead's Information Security Policies.
- Inform Data Stewards or the Audit Department about security exposures.
- Report all known breaches to the Vice President of Information Systems or other Management.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003 .

Policy 10.36 Separation of Duties

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Responsibilities must enforce a separation of duties and adhere to a "Need to know" principle. Where a separation of duties cannot be enforced by logical access controls, other non-information technology related controls must be effective.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.37 New Technology

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Information Systems strives to take the position of a "fast follower" in acquisition and implementation of new technology. We strive to be among the first institutions to offer new products and services, to leverage the Member benefit, but will not implement a system that has not been proven, sound and reliable. The risk associated with leading edge technology is greater than the Credit Union is willing to assume.

Developments in technology are monitored by IS management and staff to determine what is being developed and the performance results. Technology that has been successfully proven at other organizations will be considered for implementation at Arrowhead.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.38 Exceptions

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Because policies may be general in nature, there will be situations where economics or other considerations dictate an exception to a policy. In such situations, Executive Management may decide to accept the risk of not following an established information security policy or standard. In such cases, the senior vice president authorizing the exception must document the policy exception. The decision must be documented and should address the following areas.

- The value of the information asset, including the business consequence of its disclosure, destruction, modification, delay or misuse.
- The policy to which the exception applies.

- A description of the risk and degree of exposure that can result from the exception.
- The business reason for non-compliance.
- Any compensating controls that will reduce the risk to an acceptance level.
- Additional actions, if any, which will lead to compliance and a schedule of these actions.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.39 Employee Hire, Change and Termination Controls

IT IS THE POLICY OF THIS CREDIT UNION THAT:

New Employees
Each departmental Manager is responsible for ensuring that immediately upon hiring a new employee, Information Systems will be notified of hire date and position. New hires are to be informed of the Information Security Policy, and to sign an affidavit of understanding. Upon the form being signed, Information Systems will initiate systems access levels, commensurate with the position.

Changes to Position
When a change in position occurs, such as a promotion or transfer to a different department, the Manager of the department will notify Audit and Information Systems of the change. Audit and Information Systems will modify systems access levels, commensurate with the new position.

Termination
In the event of voluntary or involuntary termination, the terminating employee's Manager is to notify Information Systems of the termination, including the date and if possible, the time. Information Systems will ensure that all access to our systems by the employee is terminated on the termination date/time.

Arrowhead Credit Union reserves the right to terminate systems access privileges in advance of the termination date, if requested by Management.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.40 Employee Awareness and Training

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Staff play an important role in the security of member data and Arrowhead's information resources. Staff will receive training and updates on the credit union's information security policy through new hire orientation and periodic awareness training.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.41 Security Monitoring

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Compliance of Security Policy is to be monitored with appropriate controls. These controls may include physical controls (cameras, card key access), firmware controls (routers, etc.), software controls (passwords, logging processes, click streaming, etc.), or personnel controls (security guards, review processes, etc.).

Accountability for Controls over Information Systems

- Ensure that all personnel using the Credit Union's information resources are continuously aware of the importance of information assets and of their responsibilities toward protecting these assets.

- Assess the value or sensitivity of information in order to determine the protection, monitoring, and accountability required.

- Evaluate and specify control and protection requirements for information. Specify ownership. Limit physical and electronic access to information on a strict need to access basis. Authorize access based on these criteria.

- Staff shall observe controls to protect physical security and bring any incidents or practices that weaken security to management's attention.

- Clearly define the responsibilities among owners of data, users, and IS staff.

- Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the Audit or Information Systems Departments. Users are prohibited from utilizing Arrowhead Credit Union systems to forward such information to other users, whether the other users are internal or external to Arrowhead Credit Union.

Information Systems Escalation Procedures
For the purpose of ensuring the highest possible levels of system security, availability and integrity, Arrowhead will maintain current escalation procedures. Escalation procedures cover a wide scope of systems and types of processing. They will include critical system halts, application hangs, individual device (PC, printer, ATM, etc.) problems, to job processing or report output problems. The escalation procedures will clearly outline the person(s) to contact, the timeline in which to escalate a problem, and documentation of the escalation tasks performed for a given problem.

Information Capture if Computer Crime or Abuse is Suspected
To provide evidence for investigation, prosecution, and disciplinary actions, certain information must be immediately captured whenever it is suspected that a computer crime or abuse has taken place. The relevant information must then be securely stored off-line until such time as legal counsel determines that Arrowhead Credit Union will no longer need the information. The information to be immediately collected includes the current system states, as well as back-up copies of all potentially involved files.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.42 Restriction of Privacy Rights

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Areas where Electronic Monitoring May Be Used
Users may be subject to electronic monitoring while on Arrowhead Credit Union premises. This monitoring is used to measure users' performance, as well as to protect worker personal property, worker safety, and Arrowhead Credit Union property. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, locker rooms, no electronic monitoring will be performed.

Disclosure of Information to Law Enforcement
By making use of Arrowhead Credit Union systems, users consent to allow all information they store on Arrowhead Credit Union systems to be divulged to law enforcement at the discretion of Arrowhead Credit Union management.

Privacy Expectations of Information Stored on Systems
At any time and without prior notice, Arrowhead Credit Union management reserves the right to examine archived electronic mail, personal file directories, hard disk drive files, and other information stored on Arrowhead Credit Union information systems.

This examination is performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of Arrowhead Credit Union information systems.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.43 Censorship of Data

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Right to Censor Data on Organizational Systems
Management reserves the right to censor any data posted to Arrowhead Credit Union computers or networks. These facilities are private business systems, and no public forums, and as such do not provide First Amendment free speech guarantees.

Right to Remove Offense Material Without Warning
Arrowhead Credit Union retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Responsibility for Monitoring Content of Information Systems
Although Arrowhead Credit Union reserves the right to monitor and censor data, it does not have an obligation to monitor the information content resident on or flowing through its information systems.

Personal Comments on External Systems
Comments that users post to an electronic mail system, an electronic bulletin board system, or other electronic systems are not necessarily formal statements of or the official position of Arrowhead Credit Union. Users should not assume what they read or otherwise observe on Arrowhead Credit Union systems is necessarily Arrowhead Credit Union policy. Users should instead look for an indication that it is a policy statement.

Prohibition of Sexual, Ethnic, and Racial Harassment
Sexual, ethnic, and racial harassment – including unwanted telephone calls, electronic mail, and internal mail – is strictly prohibited and is cause for disciplinary action up to and including termination.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.44 Use of Personal Computers

IT IS THE POLICY OF THIS CREDIT UNION THAT:
The Arrowhead provides its employees with personal computers (PCs) and access to its network and systems. The purpose of the PCs and the network is to conduct the business of Arrowhead. Access to the network and the PCs is a privilege and may be revoked at any time. Use of the PCs constitute acceptance of this policy.

Users are expected to be knowledgeable of these and all policies of Arrowhead. Any questions should be directed to the Vice President of Information Systems. Violations of this or any other Arrowhead policy subjects the user to immediate revocation of system privileges and may result in disciplinary action including termination. Any information entered or stored on the PC or in network servers becomes the property of Arrowhead and is subject to monitoring for compliance with all Arrowhead policies by the Information Systems and Internal Audit Departments.

Username and Passwords
The user must first be authenticated through an Arrowhead-assigned network username and password and then through application or database password. Users must use an Arrowhead assigned username and password to gain access to the network. Passwords must never be shared or revealed to anyone else besides the authorized users. Personal computers must always be logged-off or locked via password protection when unattended for any significant period of time.

Design of Password
All user passwords must have at least five (5) characters. Summit passwords are alphabetic characters only. Network passwords must contain at least one alphabetic and one non-alphabetic character. Non-alphabetic permitted characters include numbers (0-9). Users are required to change their passwords every 90 days are not allowed to reuse previously used passwords.

Password Changes After Compromise
Information Systems reserves the right to change the user's password if the system is compromised or if they determine that the password does not meet specifications stated above, or if they have reason to believe the user's password has been disclosed to or discovered by unauthorized parties. The user will be notified if this occurs. If the user forgets their password and gets locked out of the system, the employee's manager should contact the IS Help Desk immediately. Users are prohibited from storing passwords in written or printed form on or near their PCs.

Limit on Consecutive Unsuccessful Attempts to Enter a Password
To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect user password must be strictly limited. If the computer system supports it, after five unsuccessful attempts to enter a password, the involved user-ID is temporarily disabled.

Network Auto Login
Auto login to the network is not allowed, unless approved by Information Systems management, since it requires user name and password to be hard coded and is a potential security risk.

Exception to Password Policies
There are some exceptions to these policies for certain user accounts. These user accounts are used for server service accounts and if the password is changed, these services will fail to start automatically, e.g. user account used for backup software, etc. All server consoles are monitored by Information Systems staff and are to be locked by a password. Auto login is allowed on certain servers because programs auto start during the login process and are dependent on auto login.

All critical system and server consoles are to be placed in a room with restricted access and are monitored by the Information Systems staff. Access to the main computer room is controlled by a security system. A magnetic security access key is programmed and issued by the Vice President Internal Audit to permit access to the Computer Room.

Unattended Personal Computers
If users leave their workstations unattended for any significant period of time, they are required to log off the network or lock their workstations to secure their computer. These time periods include, but are not limited to, breaks, lunches, meetings, restrooms breaks, and close of workday. The user is prohibited from leaving their PC unattended without logging off or locking their workstation.

Personal Use of Personal Computers and Network
As stated previously, the use of PCs in the Arrowhead network is primarily for business purposes. Incidental personal use of the PCs and the LAN/WAN is permitted. However, personal use should not interfere with Arrowhead operations, be in conflicts with other established Arrowhead policies (e.g., E-mail, Conduct, or Administrative Control Policies), nor should it cause any harm or embarrassment to Arrowhead or its members. Any personal use is expected to be on the user's own time and is not to interfere with the person's job responsibilities.

Installation of Programs
Installation of programs is restricted to Information Systems staff. Users are not allowed to download programs, games or screen savers to the hard drives on their PCs, from the Internet, internal network servers, CD-ROM drives or floppy drives.

Various departments may use third party vendors or consultants to install software or hardware. In these cases, Information Systems must be contacted prior to installation to ensure that network connections, configurations are set up correctly and that security is not compromised. If third party vendors are being considered, management should obtain a written assurance from that vendor that the software or hardware does not contain undocumented features, hidden components that may be used to compromise security. The assurance should state the system specifications and any requirements for connectivity to Arrowhead's network.

If the third party or consultant is performing the installation, IS must be contacted at the point they are configuring any connection with the network. The vendor must be accompanied at all times in accordance with Arrowhead's visitor policy.

Malicious Software (Viruses, Worms, Trojan Horses, etc.)
Introduction of virus code into any computer owned or operated by Arrowhead is strictly prohibited. Users must not intentionally write, generate, compile, copy, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of the computer's or Arrowhead network's memory, file system, or software. Violation of this policy subjects the user to immediate termination and/or criminal/civil penalties.

Arrowhead's network is protected by anti-virus software. However, virus protection software does not necessarily prevent the introduction of a virus into a computer or the network. Symptoms of a virus include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total system failure. Any user noticing symptoms such as these is to notify the Information Systems Help Desk. Because some viruses are very complex, the user should not attempt to eradicate it on his/her own. Such attempts could result in the further spread of the virus through the network. If the user is notified by virus protection software installed on the network that a virus or other malicious software is present, they are to immediately notify the Help Desk.

The virus protection software on the PC will update itself at regularly scheduled intervals when the user logs on. No user should attempt to terminate this update from occurring. If addition, users are prohibited from attempting to disable or reconfigure the virus protection software on their computer.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.45 Network Security

IT IS THE POLICY OF THIS CREDIT UNION THAT:
The Arrowhead provides its employees with personal computers (PCs) and access to its network and systems. The purpose of the PCs and the network is to conduct the business of Arrowhead. Access to the network and the PCs is a privilege and may be revoked at any time. Use of the PCs constitute acceptance of this policy.

Users are expected to be knowledgeable of these and all policies of Arrowhead. Any questions should be directed to the Vice President of Information Systems. Violations of this or any other Arrowhead policy subjects the user to immediate revocation of system privileges and may result in disciplinary action including termination. Any information entered or stored on the PC or in network servers becomes the property of Arrowhead and is subject to monitoring for compliance with all Arrowhead policies by the Information Systems and Internal Audit Departments.

Username and Passwords
The user must first be authenticated through an Arrowhead-assigned network username and password and then through application or database password. Users must use an Arrowhead assigned username and password to gain access to the network. Passwords must never be shared or revealed to anyone else besides the authorized users. Personal computers must always be logged-off or locked via password protection when unattended for any significant period of time.

Design of Password
All user passwords must have at least five (5) characters. Summit passwords are alphabetic characters only. Network passwords must contain at least one alphabetic and one non-alphabetic character. Non-alphabetic permitted characters include numbers (0-9). Users are required to change their passwords every 90 days are not allowed to reuse previously used passwords.

Password Changes After Compromise
Information Systems reserves the right to change the user's password if the system is compromised or if they determine that the password does not meet specifications stated above, or if they have reason to believe the user's password has been disclosed to or discovered by unauthorized parties. The user will be notified if this occurs. If the user forgets their password and gets locked out of the system, the employee's manager should contact the IS Help Desk immediately. Users are prohibited from storing passwords in written or printed form on or near their PCs.

Limit on Consecutive Unsuccessful Attempts to Enter a Password
To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect user password must be strictly limited. If the computer system supports it, after five unsuccessful attempts to enter a password, the involved user-ID is temporarily disabled.

Network Auto Login
Auto login to the network is not allowed, unless approved by Information Systems management, since it requires user name and password to be hard coded and is a potential security risk.

Exception to Password Policies

There are some exceptions to these policies for certain user accounts. These user accounts are used for server service accounts and if the password is changed, these services will fail to start automatically, e.g. user account used for backup software, etc. All server consoles are monitored by Information Systems staff and are to be locked by a password. Auto login is allowed on certain servers because programs auto start during the login process and are dependent on auto login.

All critical system and server consoles are to be placed in a room with restricted access and are monitored by the Information Systems staff. Access to the main computer room is controlled by a security system. A magnetic security access key is programmed and issued by the Vice President Internal Audit to permit access to the Computer Room.

Unattended Personal Computers

If users leave their workstations unattended for any significant period of time, they are required to log off the network or lock their workstations to secure their computer. These time periods include, but are not limited to, breaks, lunches, meetings, restrooms breaks, and close of workday. The user is prohibited from leaving their PC unattended without logging off or locking their workstation.

Personal Use of Personal Computers and Network

As stated previously, the use of PCs in the Arrowhead network is primarily for business purposes. Incidental personal use of the PCs and the LAN/WAN is permitted. However, personal use should not interfere with Arrowhead operations, be in conflicts with other established Arrowhead policies (e.g., E-mail, Conduct, or Administrative Control Policies), nor should it cause any harm or embarrassment to Arrowhead or its members. Any personal use is expected to be on the user's own time and is not to interfere with the person's job responsibilities.

Installation of Programs

Installation of programs is restricted to Information Systems staff. Users are not allowed to download programs, games or screen savers to the hard drives on their PCs, from the Internet, internal network servers, CD-ROM drives or floppy drives.

Various departments may use third party vendors or consultants to install software or hardware. In these cases, Information Systems must be contacted prior to installation to ensure that network connections, configurations are set up correctly and that security is not compromised. If third party vendors are being considered, management should obtain a written assurance from that vendor that the software or hardware does not contain undocumented features, hidden components that may be used to compromise security. The assurance should state the system specifications and any requirements for connectivity to Arrowhead's network.

If the third party or consultant is performing the installation, IS must be contacted at the point they are configuring any connection with the network. The vendor must be accompanied at all times in accordance with Arrowhead's visitor policy.

Malicious Software (Viruses, Worms, Trojan Horses, etc.)
Introduction of virus code into any computer owned or operated by Arrowhead is strictly prohibited. Users must not intentionally write, generate, compile, copy, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of the computer's or Arrowhead network's memory, file system, or software. Violation of this policy subjects the user to immediate termination and/or criminal/civil penalties.

Arrowhead's network is protected by anti-virus software. However, virus protection software does not necessarily prevent the introduction of a virus into a computer or the network. Symptoms of a virus include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total system failure. Any user noticing symptoms such as these is to notify the Information Systems Help Desk. Because some viruses are very complex, the user should not attempt to eradicate it on his/her own. Such attempts could result in the further spread of the virus through the network. If the user is notified by virus protection software installed on the network that a virus or other malicious software is present, they are to immediately notify the Help Desk.

The virus protection software on the PC will update itself at regularly scheduled intervals when the user logs on. No user should attempt to terminate this update from occurring. If addition, users are prohibited from attempting to disable or reconfigure the virus protection software on their computer.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.46 Remote Access

IT IS THE POLICY OF THIS CREDIT UNION THAT:
All remote access to the Arrowhead network must be authorized by the Vice President Information Systems, or credit union management, and connections must be authenticated before being established. Dial-in and VPN access are available to approved users. All users must authenticate through the dial-up server or VPN using a separate username and complex password before accessing Arrowhead's network.

The phone number of the dial-in server, VPN authentication address, user login and password should not be shared with anyone. All connections via dial-in and VPN are logged, and these logs are reviewed periodically. The remote access capability is an enhancement to our system and will be removed if abused or used for non-Arrowhead business purposes.

Vendor Extranet Leased Line Security
Vendors are able to connect directly to the Arrowhead network via leased lines. A firewall and neutral "demilitarized zones" (DMZs) are used to provide protection for internal networks from Arrowhead business partners (e.g. e-Funds and PSCU).

Arrowhead Employees & Telecommuters Dial-in Access
Dial-in access is available to all management, telecommuters and selected staff. System access through remote dial-in and VPN is controlled and authorized by a unique user name and password. All access is granted entry through a single dial-in server or VPN Internet connection.

Arrowhead Employees & Dial-out Access
Some of the applications require dial-out access to communicate with the business partners. Dial-out access is permitted and configured to use network authentication.

Support Vendors Dial-in Access
Authorized support vendors are required to dial-in through a modem server or connect via VPN to access credit union systems. Vendors are required to use usernames and complex passwords for authentication.

Exceptions

A limited number of modems exist due to DOS-based applications' inability to support network dial-out, e.g. Fed Line PC, Fannie Mae, and Zurich Payroll. Several application support vendors require direct dial-in to modems attached to their systems, e.g. HP host, AFS host, and Stratus host. Arrowhead is working with the vendors to have network dial-in and dial-out capability on an ongoing basis.

Vendors are required to call in to have the modem enabled before accessing the specific system. After the vendors are done with the support call, vendors are required to notify Arrowhead IS staff who then power off the modem.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.47 Use of Internet

IT IS THE POLICY OF THIS CREDIT UNION THAT:
Access to the Internet through the Arrowhead network is a privilege and carries responsibilities reflecting responsible and ethical use. Vice President or higher-level approval is required for all requests. Special requests must document the reasons for

requiring access to the Internet in order that IS can evaluate the resources required to maintain adequate system security. Use of the Internet through the Arrowhead network constitutes the individual's acceptance of this policy.

Employee-users are expected to be knowledgeable of these and all policies of Arrowhead. Care must be taken by all employee-users to ensure that accessing the Internet does not jeopardize member and credit union interests. Questions should be directed to the Vice President of Information Systems. Violations of this or any other Arrowhead policy subjects the employee-user to immediate revocation of system privileges and may result in disciplinary action including termination.

Authentication Process
The employee-user must first be authenticated through an Arrowhead-assigned network username and password. The username and password is the responsibility of the individual to whom it is assigned. Violations of Arrowhead Internet Use Policy and any other policy through the authorized use of the username and password subjects the individual to whom it is assigned to disciplinary action including termination. Users should not expect that transmissions made through the Arrowhead network are confidential as they are subject to review by authorized Audit and Information Systems staff for business purposes.

Monitoring Internet Use
Internet use by Arrowhead employees is monitored preventing users from going to objectionable sites. Information Systems management reviews Internet usage reports to ensure proper usage of Internet.

Personal Use
Limited personal use of the Internet is allowed by Arrowhead. However, the employee-user is reminded that use of any and all Arrowhead property is primarily for the purposes of Arrowhead business. Any personal use of the Internet is expected to be on the user's own time and is not to interfere with the person's job responsibilities.

In addition, any posting to public forums such as newsgroups, or any transmittal of electronic mail through the Internet for personal use must include a disclaimer that the views are those of the employee-user and not of Arrowhead. These forums should be used with care and not cause any adverse publicity or embarrassment to Arrowhead.

Ethical Use of Internet
At any time and without prior notice, Arrowhead management reserves the right to examine e-mail, personal files directories, and other information stored on Arrowhead computers. This examination helps to ensure compliance with internal policies, supports the performance of internal investigations, and assists with the management of Arrowhead information systems. As such, the Information Systems and Internal Audit Departments may monitor access to the Internet. Use of the Internet constitutes acceptance of such monitoring.

This policy should be read and interpreted in conjunction with all other Arrowhead policies including but not limited to policies prohibiting harassment, discrimination, offensive conduct or inappropriate behavior. Employee-users are prohibited from accessing the Internet for any unethical purposes, including pornography, violence, gambling, racism, harassment, or any illegal activity. Employee-users are forbidden or posting to public forums (i.e., newsgroups). Any electronic mail sent through or posting to public newsgroups must fall within these ethical standards.

The employee-user must abide by all federal and state laws with regard to information sent through the Internet. Arrowhead policies strictly prohibit unauthorized release or disclosure of any member information through the Internet or through any other means. Company trade secrets and confidential information should not be transmitted over the Internet. Prior approval of the Vice President of Information Systems or a higher level must be obtained to transmit any information that would be considered confidential in nature.

Employee-users are also prohibited from using Internet access through Arrowhead systems for any other business or profit-making activities.

In general, employees should exercise the same restraint and caution in drafting and transmitting messages over the Internet as they would when writing a memorandum and should assume that their messages will be saved and reviewed by someone other than the intended recipients.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.48 Downloading of Software

IT IS THE POLICY OF THIS CREDIT UNION THAT:
Employee-users are prohibited from downloading software from the Internet without prior written approval of the Vice President of Information Systems or his/her designate. Downloading of games from the Internet is prohibited. Downloading of any executable files or programs that change the configuration of your system by anyone other than Information Systems personnel is prohibited. The employee-user should take extreme caution when downloading software or files from the Internet. All files or software should be passed through virus protection programs prior to use. Failure to detect viruses could result in corruption or damage to files and/or unauthorized entry into Arrowhead's network. It is mandatory that you comply with copyright and trademark laws when downloading materials from the Internet.

If the employee-user finds that any damage occurred as a result of downloading software or files, the incident should be reported immediately to the Information Systems Help Desk.

Employee-users may not install other on-line services to access the Internet on Arrowhead-owned computers, such as America OnLine or CompuServe. Any questions should be directed to the Vice President of Information Systems.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.49 Communication Services

IT IS THE POLICY OF THIS CREDIT UNION THAT:
The Arrowhead provides its employees with communication services for the primary purpose of conducting the business of Arrowhead. These services are intended to expedite necessary Arrowhead business communication. As such, the use of telephones, voice mail, fax machines, modems, videoconferencing equipment, cell phones, and pagers are for the credit union's business purposes. Use of these services is a privilege that is warranted by the job being performed and may be revoked at any time. Use of these services constitutes acceptance of this policy.

It is the responsibility of each employee that is assigned a cell phone, pager, laptop computer, or other equipment to keep them safe and prevent any loss or damage. Lost or damaged items will require full reimbursement by the employee within 30 days of loss or damage.

Users are expected to be knowledgeable of these and all policies of Arrowhead. Any questions should be directed to the Vice President of Information Systems or his/her designate. Violations of this or any other Arrowhead policy subjects the user to immediate revocation of service privileges and may result in disciplinary action, up to and including termination. In accordance with applicable federal and state laws, any communication on these services is subject to monitoring for compliance with all Arrowhead management policies.

Business Use Voice Mail

Voice mail is assigned to employees based on the requirements of their jobs. If an individual is assigned a voice mailbox, a password will be assigned. The individual is responsible for maintaining and protecting a current password based on the policy of the credit union.

Monitoring Business Voice Communications

Business related voice calls on Arrowhead telephone lines are subject to monitoring by management for quality control purposes. Arrowhead employees are made aware of this during their orientation period and must sign a consent form before starting employment. The consent form is maintained in each employee's personnel file.

Personal Use Telephones
Arrowhead supplies telephones and voice mail for business purposes. At the discretion of management, employees may not be able to make or accept personal calls at their workstations. Personal phone calls should be made on personal time, (breaks, lunches, before and after shifts), so they do not interfere with job responsibilities.

Ethical Use of Telephones
Employees are prohibited from using any Arrowhead communication service, for any unethical purpose, including pornography, violence, gambling, racism, harassment, or any illegal activity. Users are also forbidden from using profanity or vulgarity when using communication services for business purposes. Arrowhead communication services should never be used to cause any harm or embarrassment to Arrowhead, its employees, or its members.

Employees are prohibited from using Arrowhead communication services for any business or profit-making activities, other than that of the credit union.

Disclosure of any confidential information to any party not entitled to that information is prohibited. If the employee is required to transmit member information by facsimile to a third party, the standard Arrowhead cover sheet containing a Confidentiality Notice must be used.

Special Types of Calls (International Calls, Long-Distance Calls, Calling Card Calls, 900 Number Access, etc.)

International calls (voice or facsimile transmissions) are typically the most costly calls to Arrowhead and occur on an infrequent basis. As such, access to these calls is restricted to an "as needed" basis. When the need arises to make an international call, a manager will log a request with IS Help Desk. The manager will include the reason that access is required, including the telephone number to which the call will be placed. This will allow the Telecommunications Analyst to account for these calls when reviewing the monthly bills.

- Access to international calling will be granted on a temporary basis to accommodate the request. Access will be removed by the end of the same business day that access was granted.

- Long distance and operator-assisted calls should only be for business purposes.

- Use of Arrowhead telephones to access 900 numbers is strictly prohibited. Exceptions to this policy must be approved by management, and will be restricted based on business need.

- Employees may make toll free, collect calls, calling card calls or credit card calls from the personal use phones discussed above, provided that none of the charges resulting from the call are billed to Arrowhead.

The decision to accept incoming collect calls will be determined by department management. Each department should have procedures in place to account for all collect calls accepted and to monitor compliance with those procedures. The Telecommunications Analyst should be notified whenever a collect call is accepted to ensure charges are distributed to the correct department.

Setup and Purchase of New Communication Services
The set-up of new communication services billed to Arrowhead, for use at Arrowhead and remove business sites, must be arranged through Information Systems. This includes the purchase or lease of communications devises and mediums including, but not limited to, voice, fax, data, and video circuits. Cellular phones and pagers are managed by the Facilities Department. If the need arises for anew service to be installed on a temporary or permanent basis, management must contact Information Systems. Installation of any communication services will be designed and ordered by the Information Systems Department. Information Systems will design a solution and choose an appropriate vendor to deliver the solution based on reliability, price, service and/or other operational requirements. Information Systems will then coordinate the installation of the product or service, verify its performance, approve any billing, and periodically review the design to improve performance or price.

Malicious, Threatening, Harassing or Suspicious Calls
Malicious, threatening, harassing, or suspicious calls should be reported immediately to the department manager who will then advise the Business Resumption Department. If this is not possible, the employee should take note of as many details (date, time, information showing on phone display, male or female voice, noticeable accent, age, etc.) about the caller and the nature of the call. The employee should immediately report those details to the manager upon termination of the call. Bomb threats should be handled in accordance with Arrowhead Emergency Procedures.

If an employee receives a call from anyone representing himself or herself as a telephone company employee the call should be immediately transferred to the department manager, who should report the call and all related details to the Information Systems Department. Often these calls are attempts to obtain information regarding telecommunications or to commit toll fraud. No information should be released regarding telephone numbers, voice mailboxes, access codes, etc.

Every effort will be made to identify and take appropriate action against any individuals responsible for making malicious or threatening calls.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.50 Use of Electronic Mail

IT IS THE POLICY OF THIS CREDIT UNION THAT:
The Arrowhead provides its employees with electronic mail communications. The primary purpose of the electronic mail system is to expedite necessary business communication between two or more individuals. As such, the use of electronic mail is for the credit union's business purposes. Use of e-mail is a privilege and may be revoked at any time. Use of e-mail constitutes acceptance of this policy.

Employee-users are expected to be knowledgeable of these and all policies of Arrowhead. Any questions should be directed to the Vice President of Information Systems. Violations of this or any other Arrowhead policy subjects the employee-user to immediate revocation of system privileges and may result in disciplinary action including termination. Any information included in e-mail communications becomes the property of Arrowhead subject to monitoring for compliance with all Arrowhead policies by the Information Systems and Internal Audit Departments.

E-Mail Accounts
The employee-user must first be authenticated through an Arrowhead-assigned network username and password. The username and password is the responsibility of the individual to whom it is assigned. Any authorized use of the username and password by other individuals is the user's responsibility for any and all actions of those individuals.

An electronic mail account is assigned to each employee-user. Any communication sent from this account is the responsibility of the employee-user assigned to that account. Employee-users are prohibited from allowing other individuals to send electronic mail from their account and may not use another account to send e-mail communications for their own purposes. You should not expect that electronic mail communications made through the Arrowhead system are confidential. Although users are given a username and password, this does not insulate transmissions from employer review.

Personal Use
The use of electronic mail in the Arrowhead network is for business purposes. Incidental personal use of the electronic mail system is permitted. However, the personal use of e-mail should not interfere with Arrowhead operations, nor should it cause any harm or embarrassment to Arrowhead, its members or employees. Any personal use of e-mail is expected to be on the employee-user's own time and is not to interfere with the person's job responsibilities.

Proper and Ethical Use of Electronic Mail
At any time and without prior notice, Arrowhead management reserves the right to examine e-mail, personal file directories, and other information stored on Arrowhead computers. This examination helps to ensure compliance with internal policies,

supports the performance of internal investigations, and assists with the management of Arrowhead information systems. As such, the Vice President Human Resources or any of his/her designated representatives may monitor the content of electronic mail. Use of the Electronic Mail System constitutes acceptance of such monitoring.

This policy should be read and interpreted in conjunction with all other Arrowhead policies, including, but not limited to, policies prohibiting harassment, discrimination, offensive conduct or inappropriate behavior. Employee-users are prohibited from using electronic mail for any unethical purposes, including pornography, violence, gambling, racism, harassment, or any illegal activity. Employee-users are forbidden from using profanity or vulgarity when posting electronic mail.

Employee-users are prohibited from using electronic mail through Arrowhead systems for any other businesses or profit-making activities. Disclosure of any confidential information through electronic mail to any party not entitled to that information is prohibited.

Employee-users are prohibited from entering into any contracts or agreements on behalf of Arrowhead through electronic mail. Any such contracts or agreements must be executed through normal channels and must be expressly authorized by management.

In general, employee-users should exercise the same restraint and caution in drafting and transmitting messages over electronic mail as they would when writing a memorandum and should assume their messages will be saved and reviewed by someone other than the intended recipients.

Transmitting E-mail to "All" Group

Employee-users are prohibited from sending electronic mail to all other employee-users through the use of the "All" address group unless expressly authorized by management to do so. Excessive use of this address group strains the network and subjects Arrowhead to excessive risks from computer viruses.

Electronic Mail Through the Internet

Employee-users may be authorized to transmit or receive electronic mail to and from individuals through the Internet (outside of Arrowhead's network).

Employee-users should take extreme caution when using the e-mail in this manner. All files or software should be passed through virus protection programs prior to use. Failure to detect viruses could result in corruption or damage to files and/or unauthorized entry into Arrowhead's network. It is mandatory that you comply with copyright and trademark laws when downloading materials from the Internet.

If the employee-user finds that any damage occurred as a result of downloading software or files via e-mail or any other means the incident should be reported immediately to the Information Systems Help Desk.

Misrepresenting or replacing a user identity on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.51 Software – Copyright and Maintenance Agreements

IT IS THE POLICY OF THIS CREDIT UNION THAT:
Arrowhead purchases or licenses the use of copies of computer software from a variety of outside companies. Arrowhead does not own the copyright to this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it for use on more than one computer. With regard to the use on local area networks, the software shall be used only in accordance with the license agreement.

Users learning of any misuse of software or related documentation within the company shall notify Internal Audit and the Vice President of Information Systems or his/her designate.

According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $100,000 per work copies, and criminal penalties, including fines and imprisonment. Users who make, acquire, or use unauthorized copies of computer software may be disciplined as appropriate under the circumstances. Arrowhead does not condone the illegal duplication of software.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 5, 2003.

Policy 10.52 Software – Operational Control Policy

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Client/Server and Host Parameter Changes

All requests to change any application or host or client/server system parameters must be submitted in writing with the approval by a Vice President or above. This includes, but is not limited to, share types, collaterals, hold codes, etc.

Information Systems will maintain a change control file, for the purpose of documenting change history. The change control file will contain the Vice President's approval, the specifications of the form, and the date and time the change was implemented.

Operating System Change Control
Prior to loading any new operating system releases, a change control process will be adhered to:

Included in this process will be:

- A review of the criticality of the change.
- Confirmation with critical application providers, that their software is certified for the operating system release being installed.
- Preliminary testing of the operating system and support applications in a test environment, prior to installation on production mainframes/servers.
- Performance monitoring and benchmarking where possible, to ensure that Arrowhead Credit Union systems continue to perform optimally.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.53 Software Development and Change Control

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Development Process
Application Development is the primary responsibility of the IS department. This department maintains the responsibility for understanding, adhering to, and supporting the Software Development and Change Control Policies. These policies apply to internal development staff and all third party vendors or contract developers.

Standardization
It will be Arrowhead Credit Union's practice to define and utilize IS standards wherever reasonably possible in its development process. The purpose of such standards are to assist in research of code logic, in facilitating the archival and retrieval of current and previously used program logic, and in providing time savings through efficient logic, and to reduce errors.

Development standards should include:

- File name conventions
- Job/Programming documentation conventions
- Source control standards
- Source archival standards
- Variable naming conventions
- Reasonable coding standards to facilitate readability (structure, etc.)

Use of Development Tools/Equipment
Certain tools may be utilized in the development cycle. These tools may be either software or hardware, and must be approved for use by the Vice President Information Systems, prior to use at Arrowhead Credit Union.

These tools may include test PCs and servers upon which software is to be developed, and tested prior to any code being introduced into the production environment.

Software Tools
The following software products are currently approved and in use by Arrowhead programming staff, and approved contract developers:

- Visual Studio – Visual Basic, ASP, FoxPro, C++ and similar programs.
- ODBC interface to mainframe (read only, available for authorized users only)
- Delphi software – database and applications development
- SQL Server – database development
- Macromedia Cold Fusion – application development

Hardware Tools
The following hardware products have been approved for our development process. All critical systems software must be tested on test hardware prior to being introduced on our production servers. Current test hardware is to be utilized for the purposes noted below:

- Test Credit Union: All development is to be completed and tested on this system prior to moving onto the production mainframe.

- e-Branch Staging Server: Test servers for e-branch development

- Programming PCs: Utilized for initial development and some testing.

- Programming Test Server: Server used to test server based applications, prior to moving new code to production servers (including SQL applications, etc.).

Use of Diagnostic Tools
Only personnel authorized for testing and development may use diagnostic test hardware and software, such as communications line monitors. Access to such tools (hardware or software) is to be strictly controlled and requires approval from the VP Information Systems or SVP CTO.

Change Control Process
All computer and communication systems used for production processing at Arrowhead must employ formal system development or change control procedures to ensure only authorized and tested application modifications are made. These procedures must be used for all significant changes to software, hardware, communications networks and related procedures.

Development Change Control Process will include:

- Initial work order clearly defining development requirements and development approval requirements, signed by requesting Vice President.

- Review statement by responsible Information Systems staff, to confirm functionality of the work requested is feasible.

- Initial estimate by responsible Information Systems staff of man-hours required to complete the request.

- Change Control document(s) specifying any alternations to the original work order, signed by the requesting Vice President.

- Development staff is to utilize approved development standards and practices in the design and writing of programs and will code to meet original work order specifications, and/or written change control specifications only.

- Development staff will define and utilize appropriate quality assurance and test control processes to be used in the evaluation of program completeness and integrity.

- Upon completion of preliminary development and programming test processes, the requesting department will perform a review of the development, and upon their approval, the requesting Vice President will authorize the development for production processing.

- Turnover document is to be submitted with job/program names and functional notes by programming staff indicating logic utilized to fulfill the request.

- Turnover document to be submitted to all appropriate Information Systems staff, and authorized by the Vice President, Information Systems.

- Information Systems will perform code review, verifying that coding standards appear to be in order; job/program documentation is correct; they may choose to request additional test process for operational review.

- Upon completion of Information System review, Information Systems will complete the turnover document and job/program documentation by updating the implementation dates and entering schedule references. The hardcopy turnover document will be signed by the developer implementing the new code, and will then be archived for reference in the event of a possible 'roll-back' event, or to fulfill other research requirements.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBE 15, 2003.

Policy 10.54 Third Party Vendors

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Vendor-Provided Written Integrity Statements

If procurement of third party software is being considered which is used for the manipulation of member financial data on the main computer system, management must obtain a written integrity statement from the involved vendor. This statement must provide assurances that the software in question does not contain undocumented features, does not contain hidden mechanisms that could be used to compromise the software's security, and will not require the modification or abandonment of controls found in the operating system under which in runs.

Release of System Documentation to Third Parties

Prior to being released to third parties, all documentation that describes Arrowhead Credit Union systems or systems procedures must be reviewed by the Vice President, Information Systems or higher management level to ensure that confidential information is not being inadvertently disclosed.

All contracts involving third party service providers must ensure that the third party service providers are in compliance with Arrowhead's security policies. If member data is involved, a non-disclosure agreement must be signed and annual auditing of the third party service provider for compliance must be part of the agreement.

The archival period of all Arrowhead information assets that reside at a third party must be agreed upon and approved by Arrowhead management. Such assets must be purged upon completion of use.

Disabling Unnecessary Software Features

Features which are clearly unnecessary in the Arrowhead Credit Union computing environment should be disabled at the time when software on multi-user systems is installed.

Background "Push" Updates for Software

Automatic updating of software on Arrowhead Credit Union computers via background "push" technology is prohibited unless the involved software has first been tested and approved by an authorized member of the Information Systems Department.

Prohibition of Trap Doors

Programmers and other technically-oriented staff are explicitly restricted from installing trap doors that may circumvent the authorized access control mechanisms found in operating systems and/or access control packages.

Implementation of Security Problem Fix Software

All security problem fix software, command scripts, and the like provided by operating system vendors, official computer emergency response team (CERTs), and other trusted third parties must be promptly implemented. See specific policies for specific equipment (routers, firewalls, servers, etc.).

Procedures for Rapid Roll-Back Procedures

Adequate roll back procedures must be developed for all changes to production systems software and production application software. Roll back procedures allow data processing activities to quickly and expediently revert to the prior version of such software, so that business activities can continue.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.55 Protection of Data

IT IS THE POLICY OF THIS CREDIT UNION THAT:
Arrowhead Credit Union uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these objectives, management maintains the authority to:

- Restrict or revoke any user's privileges.
- Inspect, copy, remove or otherwise alter any data, program, or other system resource that may undermine these objectives.
- Take any other steps deemed necessary to manage and protect its information systems.

This authority may be exercised with or without notice to the involved users. Arrowhead Credit Union disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.56 Intranet Content

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Ownership of Intranet Content
Unless explicitly noted on the intranet web page in question, all content posted to the intranet is the property of Arrowhead Credit Union.

Ownership of Intranet Information
All information posted to the intranet must have a designated owner. Individual departments may maintain their specific site's content.

Confidential Information on Internet or Intranet Systems
Arrowhead Credit Union confidential information must not be resident on either Internet or intranet servers unless properly protected through password-protected access.

Access to Internal Systems by Third Parties
All third party access to Arrowhead Credit Union internal computer systems which are not clearly public must be approved in advance by the Vice President of Information Systems.

Forwarding of Intranet Information
The Arrowhead Credit Union intranet is for the exclusive use of authorized persons. Unlike the Internet, information on the intranet may be disseminated only to authorized persons. Users must not forward information appearing on the intranet to third parties without going through the appropriate Internet channels (such as Human Resources, Marketing, or Public Relations).

Intranet Site Developers
All users developing intranet sites must consistently observe the intranet style guide for consistency and ease of navigation.

Disclaimer on Internet Personal Messages
Whenever a worker posts a message to an Internet/intranet discussion group, an electronic bulletin board, or another information system, this message must be accompanied by words clearly indicating that the comments do not represent the position of Arrowhead Credit Union. Such statements are required even when Arrowhead Credit Union's name does not appear in the text of the message and/or when an affiliation with Arrowhead Credit Union has not been explicitly stated. The Marketing Department will make exceptions in those instances where the message has been approved for release.

Internet Representations
When engaged in discussion groups, chat rooms, and other Internet offerings, only those individuals authorized by management to provide official support for Arrowhead Credit Union products and services may indicate their affiliation with Arrowhead Credit Union. This may be accomplished explicitly by adding certain words to their messages. Alternatively, it can be accomplished implicitly via the use of an electronic mail address. In either case, unless they have received instructions to the contrary, whenever users disclose an affiliation with Arrowhead Credit Union, they must clearly indicate that "the opinions expressed are my own, and not necessarily those of Arrowhead Credit Union."
Users must not advertise, promote, present, or otherwise make statements about Arrowhead Credit Union products and services in Internet forums such as mailing lists, news groups, or chat sessions without the prior approval of the Marketing Department.

Respecting Internet Intellectual Property Rights
Although the Internet is an informal communications environment, the laws for copyrights, patents, trademarks, and the like still apply. To this end, users using Arrowhead Credit Union systems must:

- Repost material only after obtaining permission from the source.
- Quote material from other sources only if these other sources are identified.

- Reveal internal Arrowhead Credit Union information on the Internet only if the information has been officially approved for public release.

Political Advocacy Statements on Product/Service Endorsements
Whenever an Internet user provides an affiliation with Arrowhead Credit Union,. whether implicitly or explicitly, care must e taken not to make any political advocacy statements or product/service endorsements unless the permission of the Marketing Department has first been obtained.

Unofficial Web Pages Permitted Only by Contract
Unofficial world wide web pages dealing with Arrowhead Credit Union products or services are prohibited, unless the sponsor of these home pages has a contract signed by the Marketing Department. Users who notice a new Internet reference to Arrowhead Credit Union products and/or services are requested to promptly notify the Marketing Department.

Arrowhead Credit Union E-Commerce Management Committee
Prior to being posted, all changes to the Arrowhead Credit Union e-Commerce channels must e approved by a special committee established as the eCommerce Committee. This committee will make sure that all posted material has a consistent and polished appearance, is aligned with business goals, and is protected by adequate security measures. The committee will include personnel selected by the Vice Presidents of Marketing and Information Systems.

Security and Payments Information Over the Internet
Users must not send credit card numbers, login passwords, or other security information or payments information via Internet electronic mail if it is in readable (unencrypted) form. Readable electronic mail sent via the Internet has the same security as a post card; confidential information unsuitable for a post card must not be sent by Internet electronic mail.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.57 File Downloads and Uploads

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Downloading Confidential Information
Confidential Arrowhead Credit Union information may be downloaded from the Summit System to a PC only after two conditions have been fulfilled. For this data transfer to take place a clear business need must exist and advance permission from the Vice President of Information Systems must be obtained. This policy is not

intended to cover electronic mail or memos, but does apply to databases, master files, and other information stored on mainframes, minicomputers, servers, and other multi-user machines. Exceptions to advance notice may be authorized by the Vice President Information Systems, provided the exception is noted.

Handling Software and Files Downloaded from Internet

All software and files downloaded from non-Arrowhead Credit Union sources via the Internet (or any other public network) must be screened with virus detection software. This screening must take place prior to being run or examined via another program such as a word processing package.

Reliability of Information Downloaded from Internet

All information taking off the Internet should be considered suspect until confirmed by another source. There is no quality control process on the Internet, and a considerable amount of Internet information is outdated, inaccurate, or deliberately misleading.

Uploading Software to Other Computers via the Internet

Users must not upload software which has been licensed from a third party, or software which has been developed by Arrowhead Credit Union, to any computer via the Internet unless authorization from the Vice President of Information Systems has first been obtained.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.58 Cryptography

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Technology is providing new and faster methods of transferring data between businesses and clients or members. While it is desirable to take advantage of these new technologies, our first responsibility is to maintain our members' privacy. The credit union requires encryption of member and other confidential data being transferred into or out of Arrowhead. However, this process must be managed to ensure that appropriate controls are being used, and to ensure that the encryption process does not allow other adverse effects, such as data loss.

Use of Encryption Processes

Encryption processes are required for transmittal of any member data inter-institutionally on a non-secured line (i.e., Internet). This includes, but is not limited to, human resource data, member data or brokerage information. Information Systems will maintain responsibility for all secure certificates, and all other cryptographic software applications.

Cryptographic processes must not be used for Arrowhead Credit Union information unless the Information Systems Department for the particular task first approves the processes.

Encryption Key Management

Disclosure of Encryption Keys Required

Encryption keys are a most secret type of information, and access to such keys must be strictly limited to those who have a need-to-know. Unless the approval of credit union management is obtained, encryption keys must not be revealed to staff members, consultants, contractors, or other third parties.

Miscellaneous Encryption Matters

Deletion of Readable Data After Encryption

Whenever encryption is used, users must not delete the sole readable version of data unless they have first demonstrated that the encryption process is able to reestablish a readable version of the data.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.59 Malicious Software

IT IS THE POLICY OF THIS CREDIT UNION THAT:
All staff, contractors, vendors, and any other person using or accessing Arrowhead's systems must take appropriate measures to prevent the introduction or spread of malicious software.

All PC users are responsible for updating their virus detection software by properly logging into the Arrowhead network. Intentional disabling or removal of virus detection software is prohibited and will lead to disciplinary action including termination.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.60 Hardware and Software Acquisition

IT IS THE POLICY OF THIS CREDIT UNION THAT:
All acquisitions of computer assets and software must be acquired through the Information Systems department. Software and hardware acquisition is based on business need and conforms to established configuration standards.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.61 Connectivity to External Networks

IT IS THE POLICY OF THIS CREDIT UNION THAT:
Before external services are connected to the Internet network, they must be reviewed by Information Systems and preauthorized by the Vice President Information Systems.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.62 Maintenance and Service Agreements

IT IS THE POLICY OF THIS CREDIT UNION THAT:
Arrowhead Credit Union and its employees are responsible for maintaining equipment in a responsible manner. Precautions are to be taken against abuse or negligence of all Information Services hardware.

Critical System Service Agreements
Critical systems will have hardware service agreements with 24x7 support options. Maximum response time should be four hours.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.63 Security Patch Management

IT IS THE POLICY OF THIS CREDIT UNION THAT:
Arrowhead Credit Union's servers and desktop computers must be adequately protected from internal and external threats. The credit union utilizes server, desktop and database software which are widely used and can be exploited through malicious activities. As such, these computing assets must be kept up-to-date with the latest versions and patches, and must be configured in such a way as to properly protect credit union property and information from unauthorized access. The Arrowhead patch management program specifically addresses timeframes for servers and desktop computers to be updated with applicable patches.

Server patch levels are to be logged and monitored weekly by commercially available software. Network engineers and project coordinators are directly responsible for maintaining all systems' security with oversight from the IS Director Network Support, IS Director Operations & Development, and Vice President Information Systems.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.64 Physical Asset Protection

IT IS THE POLICY OF THIS CREDIT UNION THAT:

All hardware and software used on Arrowhead's information systems and network is managed by the Information Systems department. Information Systems is also responsible for the physical inventory and maintenance of these assets.

The following are measures utilized by Arrowhead Credit Union to physically protect personal computer assets from theft, damage or unauthorized access.

- Where possible, areas containing server equipment should be locked, and keys should be registered and monitored to ensure return if an individual terminates employment. Depending on the risk and value of the system, security measures may include installation of motion detection alarms or card readers on doors accessing these rooms.

- Any equipment located in publicly accessible areas or rooms that cannot be locked should be fastened down by some physical means such as a cable lock system or enclosed in a lockable computer equipment unit or case. The equipment may have a loop through which a cable can be installed.

- Personal computers or workstations and their disks, with critical and sensitive data stored on them or accessible through them should be further secured against unauthorized use even by someone who has legitimate access to the physical space.

- Personal computers should be clearly marked with system identification tags provided by the manufacturer.

- Personal computers should be located away from hazards of the environment such as leaking water pipes. Some systems may require controlled temperature, humidity, etc., or they will not perform reliably.

- Fireproof vaults are recommended for storage of critical media.

Paper Stock Security

To reduce the risk of forgery and other unauthorized manipulations, access to Arrowhead Credit Union letter stationary, blank checks, and other negotiable items must be made available only to those persons with a demonstrable need for such forms.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.65 Computer Facility Security

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Smoking, Eating and Drinking
No persons shall smoke, eat, or drink in the raised floor area in the data center. To do so would risk electrical damage to equipment as well as risk particulate contamination to data storage devices.

Equipment Management

Alteration/Expansion of Arrowhead Computers
Computer equipment provided by Arrowhead Credit Union must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without knowledge and written authorization by the Vice President of Information Systems.

Moving Microcomputer Equipment
Microcomputer equipment (PCs, servers, etc.) must not be moved or relocated without the prior approval of the Vice President of Information Systems.

Computer Systems Belonging to Users on Credit Union Property
Users must not bring their own computers, computer peripherals, or computer software into Arrowhead Credit Union facilities without prior written authorization from their supervisor and the Vice President of Information Systems.

Off-Site Equipment Damage
Users must promptly report to their manager any damage to or loss of Arrowhead Credit Union computer hardware, software, or information that has been entrusted to their care.

Protection of Credit Union Property at Alternative Worksites
The security of Arrowhead Credit Union property at an alternative worksite is just as important as it is at the central office. At alternative worksites, reasonable precautions must be taken to protect Arrowhead Credit Union hardware, software, and information from theft, damage, and misuse.

Reporting Lost or Stolen Computers and Access Devices
Laptops that have been lost or stolen, or are suspected of being lost or stolen, must be reported to the Audit and Information Systems departments immediately. Likewise, all fobs with access to the computer room that have been lost or stolen, or are suspected

of being lost or stolen, must be reported to the Audit and Information Systems departments immediately.

Testing Physical Access Controls
Users must not attempt to enter restricted areas in Arrowhead Credit Union buildings for which they have not received access authorization.

Physical Security or Encryption of Confidential Information
All information storage media (such as hard disk drives, floppy disks, magnetic tapes, and CD-ROM) containing confidential information must be physically secured when not in use. An exception will be made if this information is protected via an encryption system approved by the Information Systems Department.

Restrictions to Magnetic Media Documentation Libraries
The magnetic tape, disk, and documentation libraries are controlled areas within the information systems department. Access must be restricted to users whose job responsibilities require their presence in these libraries.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.66 Contingency Planning and Risk Assessment

IT IS THE POLICY OF THIS CREDIT UNION THAT:

Vital Records Planning
For mission critical applications, the Information Systems department is responsible for implementing archival and retention schedules as determined by the application custodian(s). Vital records planning should be done with regard to regulatory requirements, and coordinated with workflow systems.

Steps required to implement the credit union's vital records plan include:

- Identification of all data files within a system
- Determination of the custodian of each file
- Establishment of necessary back-up frequency of files
- Establishment of retention periods for each back-up after determination of state, federal, and institutional requirements
- Consideration of automation of the vital records system, according to the size of the back-up library
- Assurances that all back-up media is viable for length of retention
- Establishment of procedures to copy back-ups to fresh media as necessary

Risk Assessment

All computer information systems and information assets must be annually evaluated by Information Systems management to determine the minimum set of controls required to reduce risk to an acceptable level.

The intention of this policy is to require a risk assessment for all production information systems, thus ensuring that critical business systems have received at least a rudimentary level of security attention. Threats and remediation steps are identified and assigned to establish risk status. Production systems are prioritized by risk, and those that present a greater risk, are examined more frequently and in greater detail. The annual risk assessment also provides background information on which management decisions such as budgets, staffing plans, and project plans can be based.

Disaster Recovery Plans for Operational Units

Each manager within Arrowhead is responsible for developing a departmental plan, making arrangements, and then testing procedures to resume normal operations within a defined period of the occurrence of a natural disaster or human act of destruction. The following items are to be included:

Critical Applications

Critical applications used by the credit union's systems need to be inventoried and updated annually. Each application is assessed from a risk perspective:

- Number of days before normal operations must resume
- Ability for manual procedures to supplant the automated system for a period of time
- Applications mission criticality
- Documentation's up-to-date status
- Identification of back-up personnel support resources

Facilities

Disaster recovery alternatives include resuming operations at a hot site, cold site or sister location. A hot site is one that is kept in a state of readiness for operations at all times and is the most expensive alternative. A cold site is one that is made ready for operations when a disaster occurs. A sister location is one similar to the site in use that can provide resources if a disaster occurs. This is generally a mutually beneficial agreement. The particular type of site chosen should be the result of a cost benefit analysis.

Items considered for establishment of a disaster recovery site include:

- Location of recovery site
- Organization of site
- Employment contract considerations
- Data communications availability

Organization
The disaster recovery plan is part of a full business recovery plan. More than likely, a disaster will affect more than the computing resources. In all dimensions of this plan, a chain of command must be clearly defined. Roles and responsibilities of computer personnel, business operations personnel, and vendor personnel must be outlined. Both the business recovery plan and computer disaster recovery plans are stored off-site and accessible potentially by an independent party.

Testing
An annual walk-through or fire drill of the disaster recovery plan is performed. Different cases or scenarios are tested. Testing documentation will be updated as needed. Critical systems must be identified and tested. Testing at the hot site must be conducted annually. Testing of end-user department applications will be tested annually.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.67 Power Failure Controls

IT IS THE POLICY OF THIS CREDIT UNION THAT:
Critical host and server computers are protected from loss of power on both short or long-term basis. Power grid configurations must be jointly designed and maintained between Information Systems and Facilities Management teams. Documentation of this grid, and the procedures required to maintain and implement it, are to be kept on file by both teams or in a central location, to facilitate routine testing and emergency implementation.

Uninterruptible Power Supply
All critical equipment is to be connected to an uninterrupted power supply (UPS) must be connected to all must be tested periodically to maintain reliability.

Backup Power Generation
A back up power generator is tied into Arrowhead's data center power system. This system is designed to automatically initiate power generation in the event of power loss to the critical power grid. Monthly testing of backup power generation is performed. Arrowhead currently utilizes a diesel generator for the purposes of emergency power generation. The Purchasing Department is responsible for ensuring appropriate levels of fuel are available and that preventive general maintenance is performed monthly on the generator.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.68 Data Backup and Restoration

IT IS THE POLICY OF THIS CREDIT UNION THAT:
A major security concern for any operation is the ability to maintain computer system availability. If the data or software is destroyed inadvertently or maliciously on a system, there must be copies of the data and software available that can be restored to allow continuation of processing with a minimum of effort on the part of the user. This requires that data and software must be copied to a separate backup medium on a regular cycle for contingent use. The backup material is kept in a location separate from the original system to protect it from the same hazards. Each site should establish appropriate backup practices, identify appropriate backup locations, and inform its constituency accordingly.

In a networked environment it is a major concern to maintain connectivity to the data center by arranging for use of alternate media and/or paths for communicating if problems arise.

Critical Systems Backup
Critical systems include Arrowhead's production mainframe, secure servers, and other business critical servers.

- Applications software should be copied to a separate backup medium as new applications are added to or on a daily basis, depending on site requirements.
- Systems software should be copied weekly and as major changes are made to system software.
- Data file copies should be created (if not already available) prior to any batch updating or daily before interactive updating. This may need to be done more frequently depending on the number and importance of transactions.
- The number of backup files and the rotation cycles should be determined as part of a system design.
- Backup materials should be stored in off-site storage with:
  - o Environmental control: safe from vandals; temperature and humidity regulated as media manufacturer recommends.
  - o Physical access: ability to access backup files as needed (24 hours/day).
- Rotation of back-up files: most current backups secured off-site; next current at secondary location; next current on-site.

Restoration
Continued compatibility requires that the backup files can be read by system hardware and software and applications software. Media degeneration implies that files should be copied to fresh media as the manufacturer recommends (for example, every two years for tape media).

Backup Operations
The following steps are included in the backup and restoration processes to assure that the correct files will be available when needed:

- Data center procedures for creating a back-up include:
  - Timing (files closed)
  - Verifying good end-of-job
  - Logging backup media appropriately
- Data center procedures for restoring files include:
  - Timing (restore is necessary and appropriate)
  - Verifying good end-of-job and error free job output
  - Proper selection of data being restored
- Appropriate data center procedures for escalation in case of problems should be in place, i.e., anomalies while back-up or restore are taking place.

PC Backups
All data on standalone computers and network clients must be backed up on a regular basis. The Information Systems department determines the frequency of backup based on how often the data changes and the importance of the data to credit union operations.

Information Systems is responsible for ensuring that files are adequately backed up and stored off-site. Information Systems is responsible for the control and backup of application software and for backup of network servers. Core systems and network servers are backed up daily.

All data storage and backups are for organizational business only.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.69 Information Security Incident Response

IT IS THE POLICY OF THIS CREDIT UNION THAT:
It is the responsibility of all credit union employees to report incidents involving suspected or actual incidents regarding information security immediately to the IS Help Desk. Information Systems staff will follow the incident response procedures when reporting any occurrence of system or information compromise, suspected fraud or system misuse to ensure proper steps are taken to identify and isolate problems, take corrective action and maintain open lines of communication with Information Systems and senior credit union management. Information Systems management will ensure the credit union complies with California SB 1386 in regards to notification of the compromise of sensitive member information.

It is Arrowhead Credit Union's policy to take a pro-active approach to Information Systems Security. However, in the event of a critical systems problem, an internal misuse of information or systems or external attacks upon our systems, we must be responsive.

Incident Reporting

All staff have a responsibility to ensure the security of computer systems they have access to and to report problems or suspected activity to the Information Systems or Audit departments immediately.

Computer security related incidents other than direct attacks will be escalated based on member or organizational impact as outlined in the incident response procedure.

Hacker Attacks

Any indication that our systems/servers are being impacted by hacker attacks, are to be reported immediately to the Vice President Information Systems, the SVP Chief Technology Officer and to the Vice President Audit. The Vice President Information Systems will appraise the situation, and determine the controls to be utilized to remove the risk (i.e. system or router shutdown).

It is the responsibility of the senior credit union management to provide appropriate notification to the CEO of the incident, and the measures of protection being taken to protect Arrowhead's systems and information.

Employee Assistance During Business Restoration

Employees are expected to be present, and to assist to the best of their abilities, with the restoration of normal business activity after an emergency or a disaster disrupts Arrowhead Credit Union business activity. After an employee's family and personal assets are determined to be safe, employees are expected to put in overtime, work under stressful conditions, and otherwise do what it takes to maintain Arrowhead Credit Union as a going concern.

Information Systems Emergency Communications

All members of the Information Systems Department who travel out of town must provide their manager with telephone numbers where they can be reached. This information must be provided in advance of the travel, and is required regardless of the reasons for travel. This policy ensures that all required staff will be readily available for emergency response and disaster recovery efforts

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

Policy 10.70 Vendor Management

IT IS THE POLICY OF THIS CREDIT UNION THAT:
All prospective vendors and service providers will be reviewed for financial stability, quality of product or service, documentation, security, and business resumption and contingency planning before selection.

Existing vendors will be reviewed periodically for service levels, product or service future direction and financial stability. Where possible, external audits such as SAS70 reports and other documentation will be reviewed on an ongoing basis to ensure vendor integrity and stability.

THIS POLICY WAS ADOPTED BY THE BOARD AND APPEARS IN THE MINUTES OF DECEMBER 15, 2003.

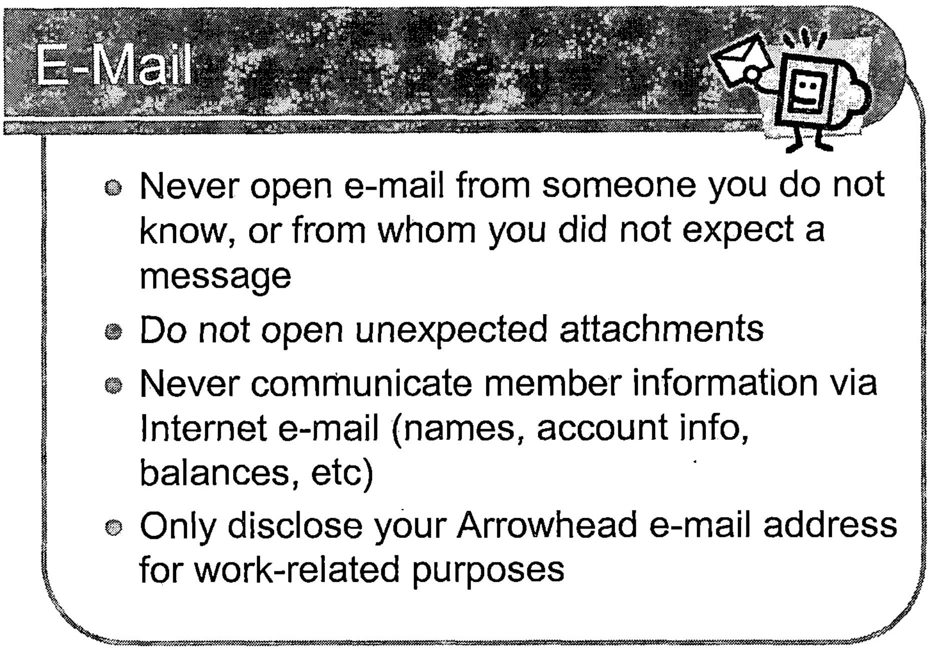
APPENDIX F

EMPLOYEE SECURITY TRAINING POWERPOINT PRESENTATION

Information Security Training Arrowhead Credit Union

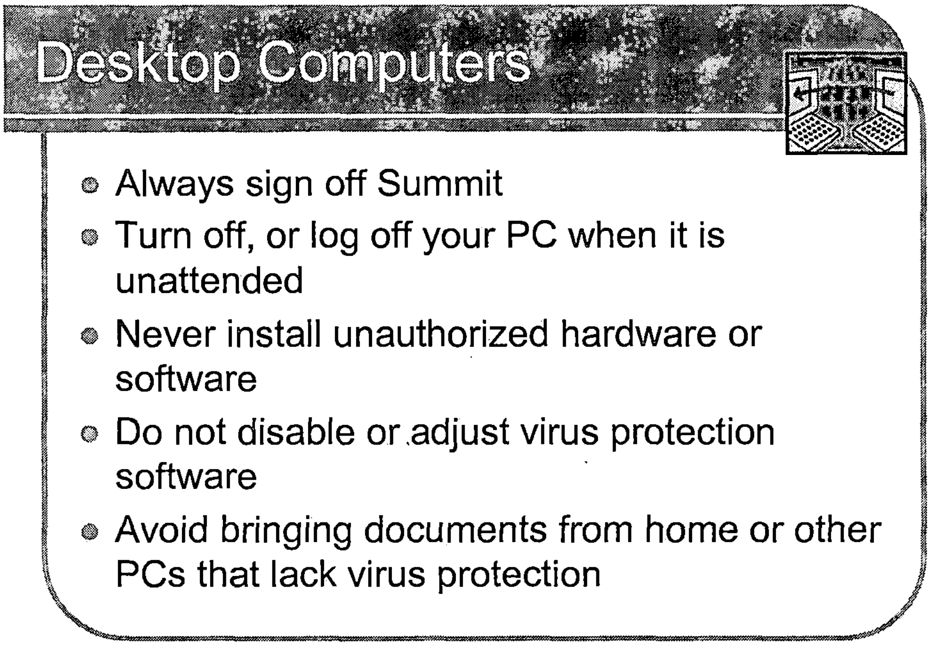
Information Security Begins With You

- Member data is our most critical asset
- Arrowhead relies on you to help keep our members' data safe
- Credit union systems are only as secure as you help make them
- Arrowhead views information security very seriously
- Legal action against the credit union can occur if member data is compromised



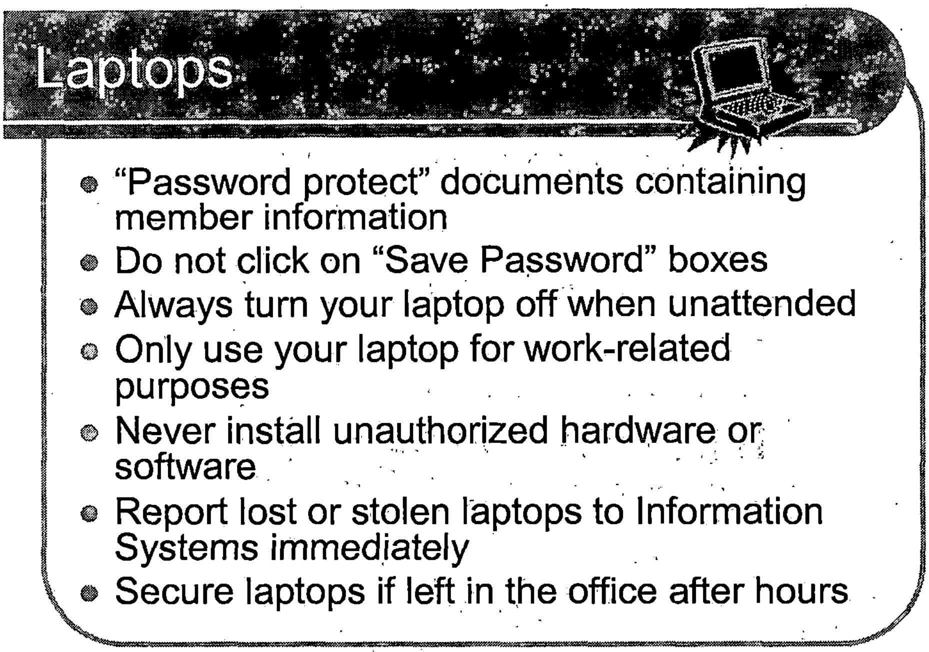
E-Mail

- Never open e-mail from someone you do not know, or from whom you did not expect a message
- Do not open unexpected attachments
- Never communicate member information via Internet e-mail (names, account info, balances, etc)
- Only disclose your Arrowhead e-mail address for work-related purposes



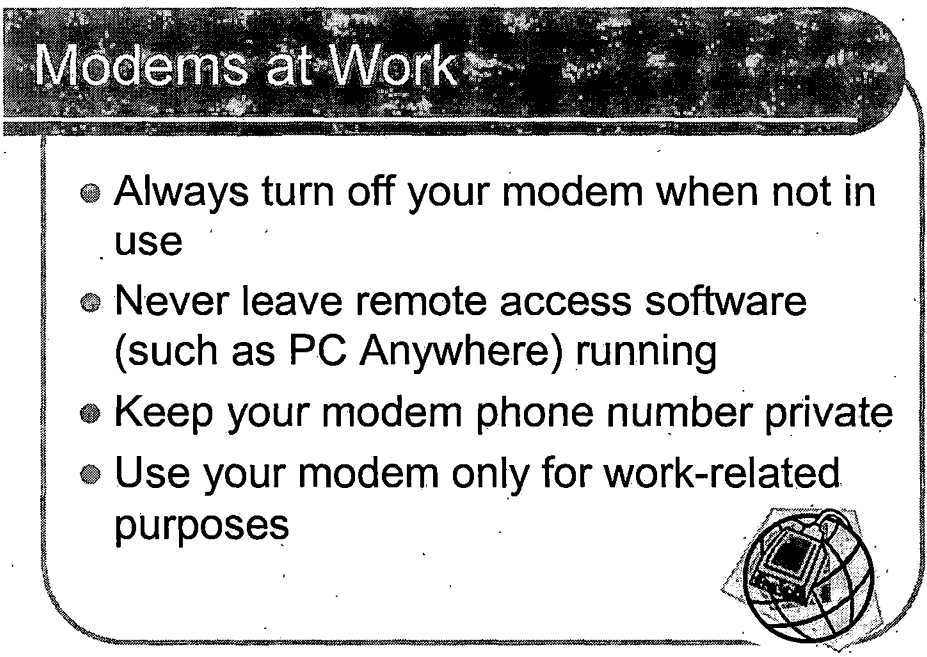
Desktop Computers

- Always sign off Summit
- Turn off, or log off your PC when it is unattended
- Never install unauthorized hardware or software
- Do not disable or adjust virus protection software
- Avoid bringing documents from home or other PCs that lack virus protection



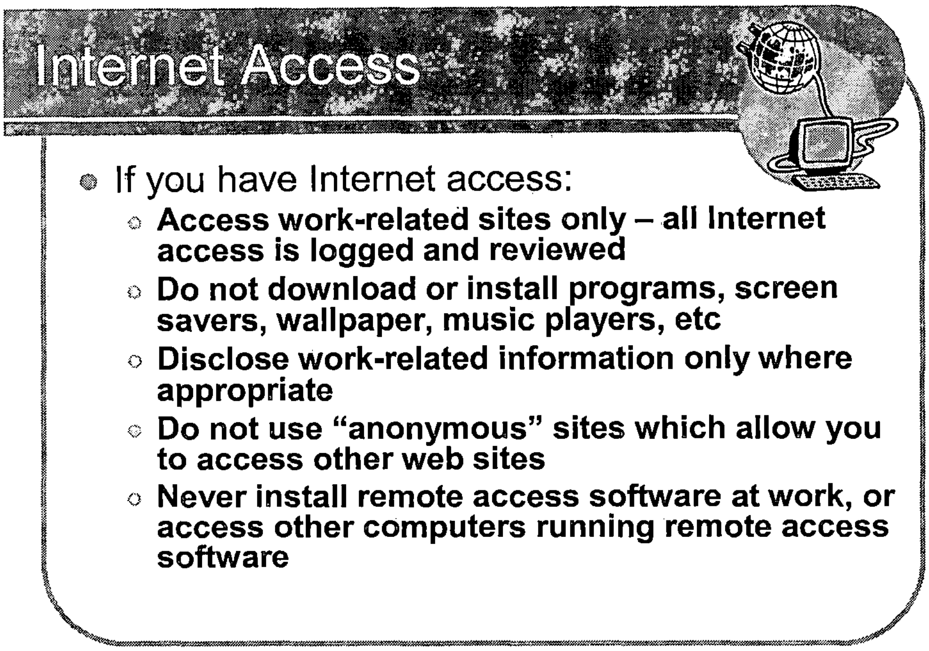
Laptops

- "Password protect" documents containing member information
- Do not click on "Save Password" boxes
- Always turn your laptop off when unattended
- Only use your laptop for work-related purposes
- Never install unauthorized hardware or software
- Report lost or stolen laptops to Information Systems immediately
- Secure laptops if left in the office after hours



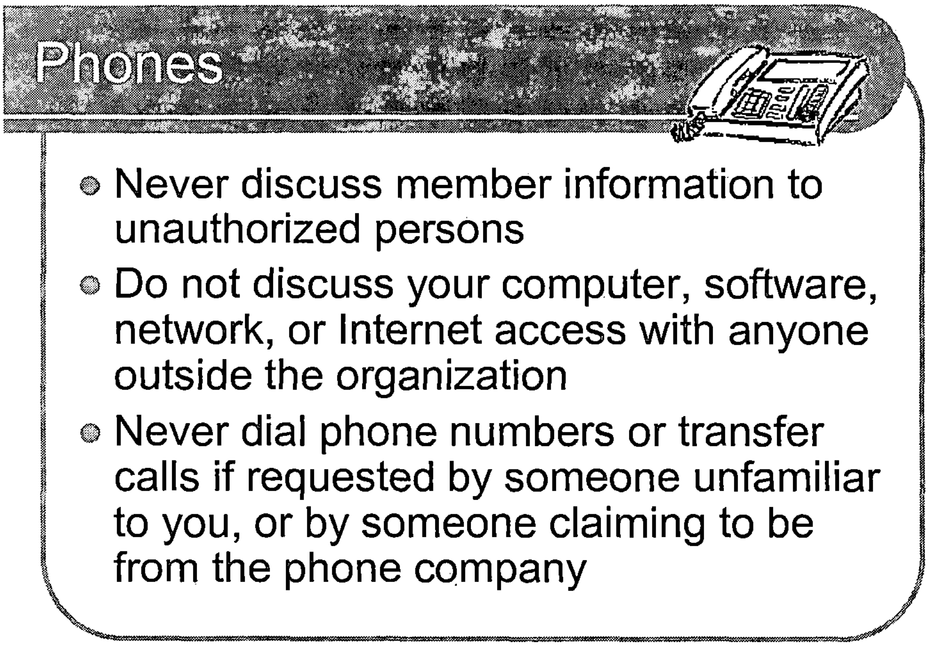
Modems at Work

- Always turn off your modem when not in use
- Never leave remote access software (such as PC Anywhere) running
- Keep your modem phone number private
- Use your modem only for work-related purposes



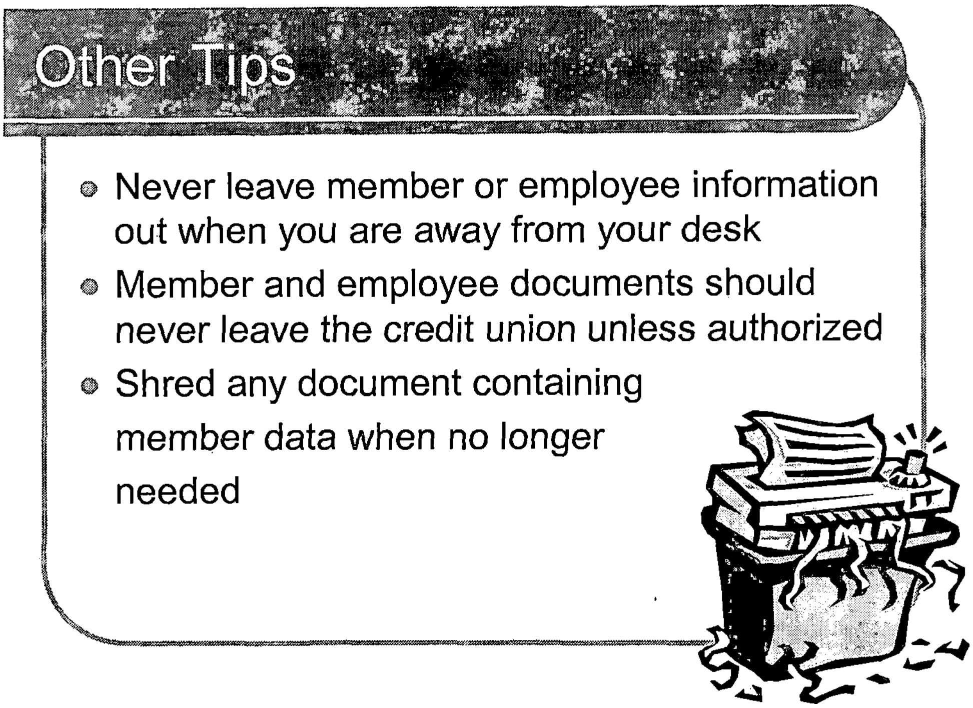
Internet Access

- If you have Internet access:
  - Access work-related sites only – all Internet access is logged and reviewed
  - Do not download or install programs, screen savers, wallpaper, music players, etc
  - Disclose work-related information only where appropriate
  - Do not use "anonymous" sites which allow you to access other web sites
  - Never install remote access software at work, or access other computers running remote access software



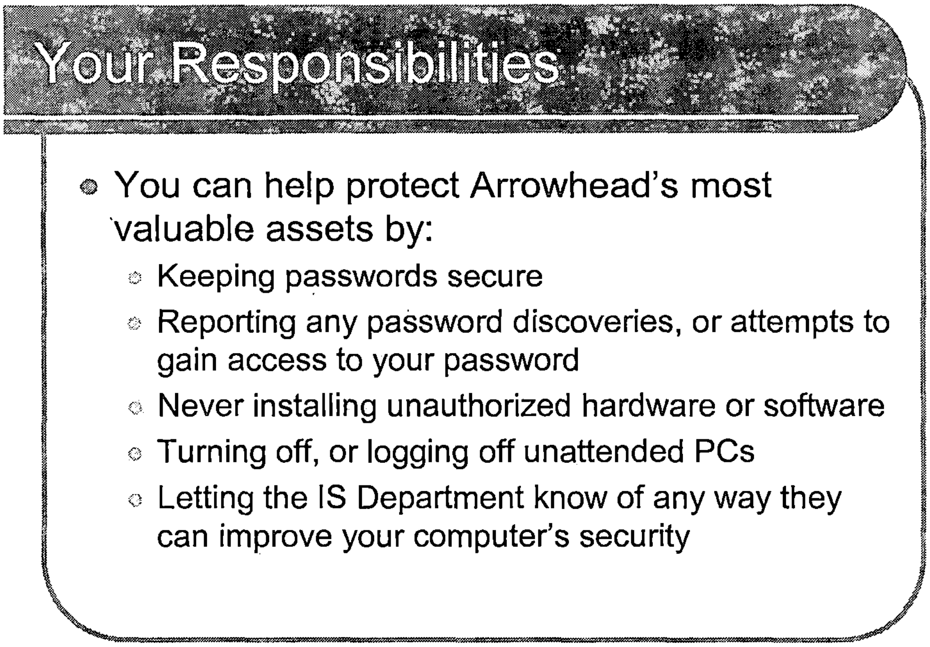
Phones

- Never discuss member information to unauthorized persons
- Do not discuss your computer, software, network, or Internet access with anyone outside the organization
- Never dial phone numbers or transfer calls if requested by someone unfamiliar to you, or by someone claiming to be from the phone company



Other Tips

- Never leave member or employee information out when you are away from your desk
- Member and employee documents should never leave the credit union unless authorized
- Shred any document containing member data when no longer needed



Your Responsibilities

- You can help protect Arrowhead's most valuable assets by:
  - Keeping passwords secure
  - Reporting any password discoveries, or attempts to gain access to your password
  - Never installing unauthorized hardware or software
  - Turning off, or logging off unattended PCs
  - Letting the IS Department know of any way they can improve your computer's security

Questions?

- If you have any questions or suggestions, please address them to your supervisor, the technology trainer, or the Information Systems department.

REFERENCES

Bong, K. M. (April 2, 2003). Conducting an Electronic Information Risk Assessment for Gramm-Leach-Bliley Act Compliance. Retrieved May 20, 2003, from http://www.johnsonintl.com/sans/risk

California Code of Regluations, Title 10. Investment, Chapter 5. Insurance Commissioner, Subchapter 5.9. Privacy of Nonpublic Personal Information. Retrieved April 12, 2004 from http://ccr.oal.ca.gov

Dollar, D. (August 2001). NCUA Letter to Credit Unions 01-CU-11, Electronic Data Security. Retried May 25, 2003 from http://www.ncua.gov/letters/2001/01-CU-11.pdf

FFIEC Information Technology Examination Handbook InfoBase. Retrieved May 25, 2003 from http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec

Financial Services Modernization Act. Retrieved April 12, 2004 from http://banking.senate.gov/conf/grmleach.htm

Foundstone. (2004). Retrieved April 22, 2004 from http://www.foundstone.com

Garfinkel, S. & Spafford, G. (1997). Web Security & Commerce. O'Reilly & Associates, Inc: Cambridge, United Kingdom.

GFI Security & Message Software. (2004). Retrieved April 22, 2004 from http://www.gfi.com

Goldenson, R. CPA. (2003). Internet Vulnerability Assessment. Clifton Gunderson, LLP: Tuscon, Arizona.

Goldensen, R. CPA. (2003). Proposal to Provide IT Consulting Services: Internet Vulnerability (Pentration) Testing. Clifton Gunderson, LLP: Tuscon, Arizona

Human Firewall. (2002). Retrieved November 15, 2002 from http://www.humanfirewall.org/issues.htm

In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act. Retrieved May 17, 2003 from. http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

Jenkins, G. (1997). Information Systems Policies and Procedures Manual. Paramus, New Jersey: Prentice Hall.

Jenkins, G. (2000). Information Systems Policies and Procedures Manual, 2000 Supplement. Paramus, New Jersey: Prentice Hall.

Ludwig, Katherine (May 1, 2003). Security Awareness: Preventing a Lack in Security Conciousness. Retrieved June 12, 2003 from http://www.giac.org/practical/gsec/Katherine_Ludwig_GSEC.pdf

McAfee System Protection: McAfee Entercept Management System. (2004). Retrieved April 24, 2004 from http://www.nai.com/us/products/mcafee/host_ips/management_system.htm

Microsoft IT Pro Security Zone. (2004). Retrieved April 15, 2004 from http://www.microsoft.com/technet/security/community/default.mspx

National Credit Union Administration Examination Resources. Retrieved February 4, 2004 from http://www.ncua.gov/IST/ExaminationResources.htm

National Credit Union Administration Rules and Regulations Part 748, Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance. (November 2001). Retrieved May 25, 2003 from http://www.ncua.gov/RegulationsOpinionsLaws/rules_and_regs/NCUA6.pdf

Office of Privacy Protection, Notice of Security Breach Civil Code Sections 1798.29 and 1798.82-.1798.84. (June 24, 2003). Retrieved May 25, 2003 from http://www.privacy.ca.gov/code/cc1798.291798.82.htm

Qualys Guard. (2004). Retrieved April 21, 2004 from http://www.qualys.com

Wood, C. (1994). Information Security Policies Made Easy. Sausalito, California: Charles Cresson Wood.