

SECURITY POLICY SECURITY MANAGEMENT

This is a copyrighted document

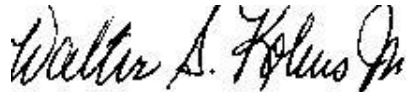
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your ORGANIZATION then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright permission. You will need to place the following documents in an envelope:

Fill out the Clearance Document and sign it; and
Fill out a check in the amount of five dollars, sign it, and make payable to TESS.

Send it to the following address: TESS, 1804 Small Ct, Raleigh NC 27612-3961. Please include your FAX number, if you have one and your mailing address so that I can send you a signed copy with both signatures.

If you are downloading multiple templates, you may include only one (1) Clearance Permission indicating the templates in paragraph 3, and a check made out in the total amount (templates X \$5.00).

Thank You,



Walter S. Kobus Jr, CISSP CISM NSA-IAM
Vice President Security Consulting Services
(919) 345-7449

CLEARANCE AGREEMENT

TESS will provide copyright license permission for use of TESS security templates (hereinafter called "Template") to _____ (hereinafter called "Recipient") for use in developing one copy of customized security documentation for the consideration of the sum of five dollars (\$5.00).

NOW, THEREFORE, in consideration of TESS Template, it is understood and agreed by and between RECIPIENT and TESS as follows:

Adaptation Right. RECIPIENT shall have the right to create an adaptation (called Derivative Works) of the Template. TESS copyright must appear on all adaptations to TESS Templates.

Performance and Display Rights. RECIPIENT may not display any TESS Templates in public in any media format.

Exclusive or Nonexclusive. RECIPIENT has nonexclusive permission of the following Template(s) _____

Term of Use. This Agreement, which is effective upon the date of its execution by the last of the signatory parties hereto, shall automatically expire and be deemed terminated effective upon the date of the happening or occurrence of any one of the following events or conditions, whichever shall first occur:

Mutual agreement of the parties to terminate the Agreement.

The expiration of a five (5) year period commencing on the effective date of this Agreement, unless such period is extended by mutual agreement of the parties in writing.

Jurisdiction. Jurisdiction of this agreement is in the State of North Carolina, United States of America. This Agreement is to be interpreted under the laws of the state of jurisdiction.

This Agreement shall inure to the benefit of and shall be binding upon both parties, its successors and assigns and shall be construed pursuant to the laws of the State of North Carolina, United States.

Total Enterprise Security Solutions, LLC

Recipient

By: _____

By: _____

Walter S. Kobus Jr., VP

Print Name: _____

Date: _____

Date: _____

TABLE OF CONTENTS

INTRODUCTION5

REFERENCES.....5

Regulatory5

Security Standards.....5

BACKGROUND5

Business and the [ORGANIZATION] Resource5

Support for Management6

PURPOSE.....6

SECURITY POLICY MANAGEMENT.....6

ASSET PROTECTION.....7

LEVEL OF SECURITY7

PROCESS FOR REQUESTING EXCEPTION TO SECURITY POLICY7

INFORMATION SECURITY MANAGEMENT PROGRAM.....7

[ORGANIZATION] INFORMATION SECURITY MANAGEMENT PROGRAM.....8

Computer Security Policies and Standards8

Access Control and Management. Access8

Network Security.....8

Disaster Recovery and Contingency Planning8

Risk Management8

Computer Security Awareness.....9

Computer Security Technology Assessment.....9

Personal Computers, Wide Area Networks (WANs), and General Support Systems.....9

Security Architecture9

ROLES AND RESPONSIBILITIES.....9

Senior Management.....10

Program and Functional Managers/Application Data Owners10

Enterprise Application Architect10

Information Technology.....10

[ORGANIZATION] INFORMATION SECURITY MANAGEMENT PROGRAM10

PROTECTION OF INFORMATION.....10

ACCOUNTABILITY11

Access to Computers.....11

System Banner11

Site Accountability.....12

Individual Accountability.....12

Privacy Accountability.....12

Passwords.....12

Use of Computer Resources.....12

Copyright Laws.....12

Concurrent User Licenses13

Risk Assessment13

Contingency Plans.....13

Data Integrity13

Communication Link.....13

Information Security Controls13

ACCESS CONTROL13

Basis for Access.....14

Discretionary Controls.....14

Identification and Authentication14

Audit Capability.....14

Access Control Systems14

Computer Security Administration14

<i>Physical Security</i>	14
<i>Application Security</i>	15
INFORMATION SYSTEMS DIVISION RESPONSIBILITIES	15
<i>Assistant Commissioner of Technology</i>	15
<i>Information Security Officer</i>	15
<i>Regional Offices</i>	15
<i>Information Security Representative</i>	16
<i>Privacy Officer</i>	16
<i>Access Control Administrator</i>	16
SEPARATION OF DUTIES	17
<i>Process Entities</i>	17
<i>Technology Entities</i>	17
<i>Constraints and Limitations</i>	17
INFORMATION SECURITY INCIDENTS	17
<i>Security Incidents</i>	17
<i>Federal Law</i>	18
<i>Kinds of Information Security Incidents</i>	18
<i>Active Prosecution</i>	18
ANTI-VIRUS MANAGEMENT	18
<i>Virus Infection Safeguards</i>	18
<i>Anti-Virus Software</i>	19
<i>Reporting Procedures</i>	19
RATIONALE	19
RISK	19
IMPACT	20
<i>User</i>	20
<i>Data Owners</i>	20
<i>Managers</i>	20
<i>Technology Infrastructure Team</i>	20
<i>Application Development/Database Administrators</i>	20

Introduction

References

Regulatory

1. Sarbanes-Oxley Act
2. Health Insurance Portability and Accountability Act.
3. Gramm-Leach-Bliley Act.
4. Social Security Act paragraphs 464 and 1137.

Security Standards

1. ISO 15408, Common Criteria, paragraph 8, Class FMT, Security Management.
2. ISO 15408, Common Criteria, paragraph 9, Class FPR, Privacy.
3. International Standard, Information technology – code of practice for information security management, ISO/ECI 17799:2000(E), paragraph 4, Organizational Security and 12.1.4, Data protection and privacy of personal information.
4. CobIT/COSO

Background

We live in an information age where computers and Information Processing Systems drive our economy, permeate our culture and help educate our people. We benefit from the increased productivity and efficiencies of using computers, yet many of us are uncomfortable with the aspect of our personal information being handled and distributed by computer systems.

Today, the Internet, cellular telephones, video cameras, credit transactions, electronic commerce and information databases put privacy at risk. Public tolerance of this invasion of privacy is based upon a feeling of “trust”. The [ORGANIZATION] has been built on the concept of “public trust”. [The need to ensure that corporate and client sensitive information, payments, point of sale, marketing, and refunds move efficiently has made the [ORGANIZATION] a trusted [ORGANIZATION]. As technology advances we find the [ORGANIZATION] dealing with new ways to process corporate information while ensuring that public trust is maintained. The need for security is apparent, but the need for an Information Security Management Program can be even more important. An Information Security Management Program provides sustainability — a consistent approach to security that can be replicated time and again across networks, applications, and transactions. The Information Security Management Program provides the following general accepted principles and practices for securing information technology systems:

Business and the [ORGANIZATION] Resource

The [ORGANIZATION] government business process requires that information be managed as an [ORGANIZATION] resource. To accomplish this, the [ORGANIZATION] has utilized three (3) levels of computer systems and application support. These are:

- Personal computer as a stand-alone unit such as laptops;
- Use of mainframe computer; and

- Network office environment which uses business tools and applications and is supported both in an internal and external work environment.

Support for Management

These systems operate at corporate offices and sites in [list corporate offices and site] supporting the [ORGANIZATION] business applications dealing directly with customer and clients. The information used by these systems is often sensitive and/or [ORGANIZATION] critical and requires protective measures. Also, it is often transmitted through a telecommunications network for additional processing. This flexibility creates vulnerabilities for the [ORGANIZATION].

Purpose

To provide a statement of [ORGANIZATION] policy on the establishment of an Information Security Management Program. This policy:

- Establishes responsibilities for protecting the [ORGANIZATION] information assets relating to computer-stored and processing data, computer equipment, and computer software;
- Provides for the implementation of adequate security measures for preventing misuse and loss of the [ORGANIZATION] information assets;
- Establishes the basis for audits and risk assessments, and for preserving the [ORGANIZATION]'s management options and legal remedies in the event of information asset loss or misuse;
- Establishes Information Security Awareness training in the [ORGANIZATION] to educate, train, and professionalize the workforce in Information Assurance, knowledge, skills, and abilities. Subsequent training to Application and Data Owners, include information systems security, as well as the additional measures and controls to protect information and information systems upon which information is processed, stored, and transmitted against denial of service, unauthorized disclosure (accidental or intentional), modification, or destruction; and
- Applies to the [ORGANIZATION] sites and regular full-time, regular part-time employees, contractors, consultants, and temporary state employees.

Security Policy Management

The Manager, Information Security Service Department, referred to as the Information Security Officer, has primary responsibility to identify, recommend, and implement appropriate cost-effective security measures to protect the [ORGANIZATION] information assets. [ORGANIZATION] information is an asset and is protected, in all of its forms, from accidental or intentional, but unauthorized disclosure, modification, destruction, or the inability to process that information. Use of [ORGANIZATION] information is sensitive and is allowed only as necessary to support authorized business activities.

Asset Protection

Information systems, computer equipment, and related corporate data are vital [ORGANIZATION] assets requiring protection appropriate to their value. Managers must protect these assets against accidental or unauthorized use, modification, disclosure, or destruction. They must also ensure their security, reliability, integrity, continuity of operations, and compliance with Federal laws and regulations.

Level of Security

The security policies described in this policy are the minimum uniform measures to be applied to information processing systems. Individual Directors and Managers are not prohibited from applying controls that are more stringent. Additional measures should be undertaken to mitigate any security risks that would enhance protection of the [ORGANIZATION] information assets and maintain public trust. Security policies are intended to protect information processed by computers. This includes all computer equipment, peripherals, programs, data, associated documentation, contractual services, personnel, supplies, and facilities.

Process for Requesting Exception to Security Policy

Very few policies stay unchanged forever. The success of the security policies depends on the users and business culture. Changes to policy can result from two different sources.

- If a manager determines that compliance with a particular security policy would result in substantial loss of efficiency and/or productivity or would be incompatible with existing policy, the manager may request approval to deviate from that security policy requirement; and
- If a manager determines that a security policy needs to be updated, removed, or added, the manager may submit an “exception request” to the Information Security Officer.

Each request shall be in writing through channels to the Information Security Officer. Included in each request shall be a statement detailing the reasons for the exception and compensating controls. Requests for exception shall be evaluated and decided upon by the Information Security Officer or the Executive Steering Committee and the requested party informed of the action taken. An approved exception that involves a deviation to policy shall only be granted for a time period not to exceed six (6) months.

Information Security Management Program

The Chief Information Officer is charged with administering the [ORGANIZATION] Information Security Management Program. Primary security responsibility for data or information systems is held by the Executive Managers, Data Owners, or those individuals charged with managing information systems. Secondary responsibility is vested in employees or other users authorized to access to [ORGANIZATION] data or systems. The Information

Security Service Department is charged with development, implementation, and evaluation of the [ORGANIZATION] Information Security Management Program.

[ORGANIZATION] Information Security Management Program

The [ORGANIZATION] Information Security Management Program is divided into the following security management sub-programs:

Computer Security Policies and Standards

The Information Security Service Department is the [ORGANIZATION]'s computer security policy-making group responsible for the creation, evaluation, and administration of computer security policy, guidelines, and procedures in support of the [ORGANIZATION] security program.

Security Certification and Accreditation Program

A system must be secured at a level appropriate to its data classification to the [ORGANIZATION] and to comply with mandated security requirements. This level of security is based on a determination of sensitivity and criticality made by the Data Owner by classifying the information to be processed and evaluating whether the application is critical to the [ORGANIZATION] operation. The Data Owner of a system is responsible for ensuring that security issues are addressed in the early phases of the system development life cycle.

Access Control and Management. Access

Systems, data, and information must be controlled and secured at a level appropriate to its data classification and in compliance, which could cause employees, managers, and executives to be individually fined or dismissed. It is the responsibility of all employees and contractors to safeguard systems, data and information at the appropriate level categorized by management regarding the sensitivity of information and criticality of the [ORGANIZATION] systems.

Network Security

A telecommunications network must be secured at a level appropriate to its data classification to the [ORGANIZATION] and mandated requirements. It must also be reliable and available for use by the [ORGANIZATION]. The Information Security Service Department provides consulting, monitoring, and comprehensive, enterprise quality information security solutions support for the [ORGANIZATION] network. These activities include evaluating network architecture and firewalls, providing encryption and Intrusion Detection Systems solutions, reviewing business partner connectivity, and WEB application servers.

Disaster Recovery and Contingency Planning

All applications defined by Data Owners as critical to their operations must be supported by an up-to-date, tested contingency plan. The Information Security Service Department provides consulting and solution support in this area.

Risk Management

All managers must assess the vulnerabilities and risks of both general support systems and field sites in order to develop and implement cost-effective security measures.

Computer Security Awareness

All employees must have awareness of their computer security responsibilities relative to the use of computers, general support systems, and information being processed. This includes the safeguarding of logon IDs and passwords, physical security of computer equipment, and protection of sensitive information.

Computer Security Technology Assessment

The [ORGANIZATION] must keep abreast of changes in computer security technology and make recommendations for the deployment of the new technology in a responsible manner. The Information Security Service Department evaluates and recommends security products for implementation.

Personal Computers, Wide Area Networks (WANs), and General Support Systems

A security program has been implemented that provides basic security protection for personal computers, WANs and general support systems at a level appropriate to their value to the [ORGANIZATION] and mandated security requirements.

Security Architecture

Security architecture is required to protect the [ORGANIZATION] information processing systems containing sensitive information. The Information Security Service Department is responsible for managing and developing this architecture.

- *Personnel Security.* Clearances must be obtained for persons in sensitive positions. Executive Management's responsibility is to ensure that data processing-related positions meet the security guidelines established by the [ORGANIZATION] and that all information systems-related positions requiring sensitive clearances are identified and that clearances are kept current.
- *Physical Security.* Computer equipment, data, facilities, and information must be safeguarded at a level appropriate of its data classification to the [ORGANIZATION] and mandated security requirements. The Facilities Security Officers, who are not to be confused with an Information Security Officer Professional, are responsible for both facility physical security and personnel security. Due to a potential conflict of interest, individuals cannot be assigned both duties. The Information Security Service Department and Facilities Security Officers must work closely with each other to ensure both the protection of individual, privacy of information, and physical security requirements for computer rooms are met.
- *Computer Security Audit, Evaluation, and Review.* The Internal Auditor is responsible for auditing [ORGANIZATION] information systems and performs developmental audits of automated systems, audits of operational and financial systems, and environmental audits. The Information Security Service Department performs operational security compliance reviews of computer systems and/or computer sites.

Roles and Responsibilities

Senior Management

Managers at all levels must provide for the computer security needs under their jurisdiction. They must also ensure that all reasonable actions are taken to guarantee this security and that problems, requirements, and matters requiring establishment of policy related to computer security are raised to the highest level necessary for resolution. Managers who have the role of Data Owner must ensure that information is properly classified and protected. In addition, the Data Owner will:

1. Ensure that the staff is aware of the need for security and develop any additional local guidelines and procedures for the staff to follow;
2. Determine whether the level of security provided for a system is appropriate to its data classification and in compliance with mandatory security requirements;
3. Ensure that the [ORGANIZATION] security policy, guidelines, and procedures are followed in all system activities, including development, and operation;
4. Provide the resources to enable employees to carry out their responsibilities for securing information and related resources; and
5. Assign overall information protection responsibility.

Program and Functional Managers/Application Data Owners

A Data Owner, as owner of an Information System Program, must assign a functional system coordinator to each owned program to authorize, control, and monitor all access requirements associated with the program. The Data Owner must delegate this authority in writing.

Enterprise Application Architect

The Enterprise Application Architect is responsible for ensuring that all architectures, regardless of origin, have security appropriate to its value to the [ORGANIZATION] or because of legal requirements. The Enterprise Application Architect shall ensure that all architectures and applications that require security Certification and Accreditation are identified to the Information Security Officer so that a certification team can be formed. The certification team shall be responsible for developing the security profile of requirements that the architectures must meet to ensure their security, reliability, integrity, continuity of operations, and compliance with mandatory security requirements. Architectures not requiring Certification and Accreditation still require some level of security protection. The Enterprise Application Architecture shall coordinate with the Information Security Officer on these architectures to ensure that the appropriate level of security requirements are identified and in place.

Information Technology

Security professionals, administrators, technical consultants and security auditors shall assist management in the administration of the Information Security Management Program to identify business needs and limit access to information on a “need to know” basis.

[ORGANIZATION] Information Security Management Program

Protection of Information

To make its official records available to the public to the maximum extent required by the public interest, and to ensure the security, confidentiality, and integrity of official records containing

sensitive information, it is the policy of the [ORGANIZATION] to maintain definitive and uniform information security safeguards. These safeguards will have as their purpose:

- Ensuring the effective operation of the [ORGANIZATION] through appropriate controls over sensitive information; and
- Protecting personal privacy by limiting unauthorized access to sensitive corporate information.

Accountability

Access to Computers

Access to computers is established at the site and/or individual user level.

System Banner

All computer systems will have a banner that all users will view before logging in or signing on. The following banner must be implemented on all computer systems and platforms within the [ORGANIZATION]. This banner must be presented at entry to any platform, at initial logon or initial connection. The user must take overt action to proceed to the next screen. This can be accomplished by pressing a key on the keyboard or by clicking a mouse button. The purpose is to ensure the user has accepted the information on the screen and acknowledged their rights and responsibilities before proceeding into a [ORGANIZATION] network or system. No changes to this banner are permitted without the Information Security Officer and Legal approvals.

The only exception to implementing this banner is for WEB pages, since each WEB page is required to present it's own warning for all users, approved in advance by the Information Security Service Department and Legal.

BANNER OF ALL LOGON COMPUTER PLATFORMS

“WARNING! FOR OFFICIAL USE ONLY ...

This is a [ORGANIZATION] system and is intended for official use only. Unauthorized access is prohibited. All user activities are subject to monitoring in accordance with the [ORGANIZATION]'s policies to ensure compliance with Tax Information Security Guidelines for Federal, State, and Local Agencies, IRS Publication 1075, dated June 2002, and State laws. Copies of the [ORGANIZATION]'s policies on use of the [ORGANIZATION]'s computers communications systems may be obtained from the system administrator or from the [ORGANIZATION]'s web site.

YOU HAVE NO EXPECTATIONS OF PRIVACY USING THIS SYSTEM. Authorized employees have the right to examine active and stored e-mail and files within all systems. Others may inadvertently view your messages. Users are responsible for the images they cause to be displayed on, and the contents of, messages transmitted over the [ORGANIZATION]'s systems. All communications are to follow the proper business etiquette, avoid insensitive, hostile, or offensive subjects and language that would violate

official [ORGANIZATION] policies and standards. The unauthorized release or use of the [ORGANIZATION] information is prohibited.

Non-compliance with any of these conditions is grounds for disciplinary action up to and including removal or termination, as well as criminal prosecution. Report instances of suspected misuse to your supervisor or systems administrator.”

Site Accountability

Site accountability is established through issuance of a site ID. A site ID must be limited by system hardware or software such that access is restricted to a unique system/network/terminal address. Site IDs may only be issued to devices that are in a physically controlled environment and where user activity is directly supervised either locally or remotely. Use of site IDs is appropriate for controlling access by unattended devices or for terminals that must be in continuous use.

Individual Accountability

Individual accountability is established through issuance of a logon ID/user account that is documented with the manager approval and the approval of the Data Owner, if appropriate. For the purpose of this policy, all references to logon ID and user account are grouped under the term logon ID. Access is authorized by completion of a request for computer access. Access to computers is controlled and subject to scrutiny, including material accessed and actions taken. Managers at all levels are responsible for any disciplinary or adverse actions against employees with active logon IDs or other access to computers. Managers are also responsible for completing and routing a security incident report for all security incidents.

Privacy Accountability

To protect the privacy of corporate information, Data Owners shall approve and grant authorized access on a “need-to-know-basis”. Data Owners shall have the responsibility to inform the *Privacy Officer* about any proposals to keep personal information in a structured file, and to ensure user awareness of the data protection principles defined in policy, State, and Federal Laws.

Passwords

Passwords must be used in conjunction with logon IDs assigned to individuals. Passwords will conform to standards published.

Use of Computer Resources

Computer equipment, computer software (including vendor-licensed, shareware, freeware, and the [ORGANIZATION]-developed), and data files are the property of the [ORGANIZATION]. Use is restricted to official purposes and, except when authorized; The [ORGANIZATION] computer equipment may not be used for personal purposes.

Copyright Laws

All employees and contractors must comply with copyright and reproduction laws, proprietary computer agreements and reproduction agreements applicable to the software used in the normal course of their business. Failure to exercise the proper care, making copies for other than backup purposes, or the illegal distribution of copyrighted software can result in disciplinary action. It is

strongly recommended that when any software is procured for distribution under a license agreement with a vendor, all the [ORGANIZATION] employees and contractors must be made aware that such an agreement to copy and distribute the software exists. Ways that can be used include labeling the disks with the contract or license number, storing either the original disks or documentation in a safe place, or the metering of software on a local area network to control use.

Concurrent User Licenses

All employees and contractors must comply with concurrent user license agreements. Failure to comply with these agreements may result in disciplinary action.

Risk Assessment

All elements or components of critical computer systems must function in a cohesive, identifiable, predictable, and reliable manner so that malfunctions can be detected and corrected. A risk assessment must be conducted every three years for critical computer and sensitive application systems. This assessment must be made a matter of record and retained on file until a subsequent risk assessment is performed.

Contingency Plans

Each computer site must develop a site contingency plan. All critical application systems must have an individual application contingency plan. Contingency plans will be developed in accordance with Disaster and Contingency security policy. Use of the [ORGANIZATION] recommended disaster planning software tools are strongly recommended. For information on what tools are available, contact the Information Security Officer. Contingency plans will be tested every two years upon success of initial testing. A detailed record of the test exercise, its results, and follow-up action must be maintained until completion of a subsequent test.

Data Integrity

Each file or collection of data in a computer system must have an identifiable origin and use. Accessibility, maintenance, movement, and disposition of the data are governed on the basis of its sensitivity.

Communication Link

Communication links and lines must be secured in a manner appropriate for the information being transmitted.

Information Security Controls

Information requires some level of protection to prevent accidental or unauthorized access, disclosure, modification, or destruction. However, sensitive information requires additional security controls because of its value to the functioning of the [ORGANIZATION] or because of legal or contractual requirements. Such safeguards protect the interests of the [ORGANIZATION], its employees, its contractors, and the general public.

Access Control

Basis for Access

Access to sensitive information must be based on the user's need to know. "Read" access to non-sensitive information will be restricted upon written request by the Data Owner or designee. Access to all system resources and capabilities must be based on the concept of least privilege; that is, access to the lowest level of computer capabilities necessary to perform the user's duties. Access will be managed and controlled using software/hardware that provide, as a minimum, discretionary access controls, identification and authentication, and audit trails.

Discretionary Controls

Discretionary access controls define and control access between named users and named objects (e.g., files and programs). These access controls shall be capable of including or excluding access to the single user level.

Identification and Authentication

Identification and authentication shall require users to identify themselves to the operating system prior to allowing the user to perform any other actions. The operating system shall be able to enforce individual accountability by providing the capability of identifying each individual computer systems user and associating that user with all actions taken by that user.

Audit Capability

The system shall have the audit capability to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The system will have the ability to selectively audit the actions of any one or more users based on individual identity. See Security Audit Policy 200 and guidelines for further information on audit trails.

Access Control Systems

Specific computer systems may necessitate the use of an approved access control package. The Information Security Officer is the approving authority for access control systems.

Computer Security Administration

If a Field Service Office or site does not have a designated security officer, the manager of a facility must designate an Information Security Representative to perform the computer security administration. Managers must assure that the requirement for a separation of duties is met when assigning personnel to perform the security functions. The person appointed to perform the Information Security Representative function is responsible for computer security administration at the field service office or site.

Physical Security

Computers must be protected from unauthorized personnel. Security measures must reduce exposure to physical threats that could adversely affect computer services or support. Concerns relative to physical threats and accessibility by unauthorized personnel should be escalated to the Information Security Officer.

Application Security

The use of embedded logon IDs or logon IDs maintained in-line (in application code or batch files, stored in application files, tables, etc.) to control application level security is prohibited. Any deviation from this policy requires a waiver issued by the Information Security Officer.

Information Systems Division Responsibilities

Assistant Commissioner of Technology

Authority for implementation and management of an Information Security Management Program is delegated to the Assistant Commissioner of Technology. The Assistant Commissioner of Technology is responsible for technical guidance for information protection, planning for contingencies for computer processing, security of data stored on computer equipment, telecommunications, and computer software security.

Information Security Officer

The Information Security Officer is responsible for development and coordination of the [ORGANIZATION] Information Security Management Program. As such, The Information Security Officer develops and manages implementation, execution, and review of computer and telecommunications security programs for the [ORGANIZATION] as follows:

1. Administer the Information Security Management Program and ensure its management is in accordance with security policies;
2. Approves requested deviations or revisions to procedures to security policies;
3. Conducts risk assessments at the direction of the Assistant Commissioner of Technology;
4. Establishes training requirements for computer security and monitors computer security training as necessary;
5. Conducts periodic surveys of facilities support offices using computer equipment to evaluate effectiveness of computer security controls and advises management of problems and trends found;
6. Provides solutions, guidance and expertise in computer security;
7. Maintains awareness of the security status of sensitive and critical automated systems;
and
8. Ensures that computer security policy is effectively implemented, by:
 - a. Preparing, disseminating, and maintaining plans, instructions, and standard operating procedures for computer security; and
 - b. Assisting in and/or conducting reviews.

Regional Offices

The term Regional Office manager as used here refers to the manager who is responsible for computer security at the Corporate Regional Office. The responsibilities of the Regional Office manager include:

1. Ensuring that the office complies with all computer security requirements, with the exception of approved deviations and any periodic changes in the [ORGANIZATION] policies;

2. Ensuring that all employees who use or are associated with the computer equipment are provided security awareness training appropriate to their responsibilities;
3. Designating a permanent employee as an Information Security Representative;
4. Coordinate with the Information Security Officer on computer security violations, which are either suspected or confirmed, and actions taken;
5. Taking appropriate action against employees who violate Information Security Management Program security policies, or procedures; and
6. Coordinating the security indoctrination and training sessions for new or assigned personnel using computers.

Information Security Representative

Each manager of a Division, Regional Office, Unit, or Group shall designate at least one person as the Information Security Representative. The Information Security Representative performs an ad-hoc responsibility in conjunction with assigned duties. Responsible for managing security, the Information Security Representative may receive technical guidance from The Information Security Service Department. All Information Security Representatives must be designated in writing. The Information Security Representatives' duties may encompass the following:

1. Ensure that computer audit trails are used to provide for internal security audits or tests, if the capability exists;
2. Ensure that security requirements and instructions are issued and distributed.
3. Provide security information to the Information Security Officer as requested;
4. Recommend that protective controls be implemented to prevent unauthorized access to computer systems and data;
5. Ensure that current records of all security incidents involving computer systems are generated and that appropriate actions are taken to prevent recurrence; and
6. Ensure that system backups are performed on sensitive information located on workstation and laptops on a scheduled basis.

Privacy Officer

The privacy officer provides guidance on:

1. The requirements of State and Federal Privacy laws;
2. Disclosure of and access to sensitive information; and
3. Security and protection requirements in conjunction with the information processing system when there is some overlap among sensitivity, disclosure, privacy, and security issues.

Access Control Administrator

The Access Control Administrator shall be responsible for the following assuring the following access controls:

1. Access is auditable and responsible to a single individual;
2. A separation of duties is maintained;
3. Access is approved by the Data Owner, if appropriate; and
4. Access control procedures and processes are in place:

- a. Ensure that User's can be associated to an approved access control form signed by the User manager; and
- b. Access to sensitive information has the approval of the appropriate Data Owner(s).

Separation of Duties

To protect the [ORGANIZATION] information assets, critical business processes must be performed by separate entities (individuals or groups). Management must enforce appropriate separation of duties in order to protect the [ORGANIZATION] information assets.

Process Entities

The following processes must be assigned to separate entities:

1. Data entry
2. Data verification

Technology Entities

The following technology processes must be assigned to separate entities:

1. Application development
2. Customer acceptance testing
3. Production Operations
4. System software development, implementation and maintenance
5. Security administration

For example, application programmers must not have Write access to production information.

Constraints and Limitations

When constraints or limitations of the [ORGANIZATION] (such as may be imposed by human resources) prohibit a complete separation of duties, compensating controls such as the following must be implemented:

1. Increased supervisory review;
2. Reduced span of control;
3. Rotation of assignments; and
4. Independent review, monitoring and/or auditing.

Information Security Incidents

All known or suspected [ORGANIZATION] information security incidents must be reported immediately to the Information Security Officer (Exhibit A).

Security Incidents

An Information Security Incident must be reported and the attached form completed if someone:

1. Reads, changes, copies, uses, discloses or destroys any information that has not been authorized by the [ORGANIZATION] management;
2. Falsifies or uses information assets in the commission of a crime;
3. Introduces malicious code, tampers with, interferes with, or gains unauthorized access into any the [ORGANIZATION] system or network; and
4. Steals, damages or destroys the [ORGANIZATION] information assets.

Federal Law

The Federal law requires agencies to report and promptly investigate all incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, or access to automated files and databases, as well as incidents involving loss, damage, or misuse of information assets, including hardware. If the incident constitutes a criminal act, the appropriate law enforcement agencies will be notified.

Kinds of Information Security Incidents

There are many different kinds of information security incidents. Some are planned criminal activities (e.g., Stealing a [ORGANIZATION] personal computer); others are the result of complacency, carelessness or improper training (e.g., Sharing confidential member information without permission). In many situations, the individual plays an active role in the information security incident (e.g., Using another person's User ID and password to access privileged information), while in other situations the individual may actually be the victim (e.g.: Finding a virus on their computer system). For examples of information security incidents, refer to the Information Security Incidents - Staff Procedure.

Active Prosecution

Unauthorized access, use, disclosure or malicious destruction of information is subject to prosecution under appropriate legal statutes found under the "Regulatory" paragraph in the front page of this policy. The [ORGANIZATION] will actively pursue prosecution and/or adverse action against anyone that accesses, uses, discloses or destroys the [ORGANIZATION] information assets in an unauthorized manner.

Anti-Virus Management

The [ORGANIZATION] will ensure that virus detection software is used on all computer systems to detect and remove software viruses.

Virus Infection Safeguards

To minimize computer virus infections, the [ORGANIZATION] staff shall adhere to the following safeguard policies:

1. Employees throughout the [ORGANIZATION] must ensure electronic media is virus free;
2. Diskettes will be scanned using a current version of the [ORGANIZATION] authorized virus detection software before use. This includes diskettes from co-workers and vendors;
3. Employees will not download executable programs or files from on-line bulletin boards, the Internet, or services without Information Security Officers approval;

4. Software must be checked by an [ORGANIZATION] approved virus detection software program prior to installation. Software on diskette should be write protected after a successful virus scan and before installing the software to prevent subsequent infection from a contaminated machine; and
5. The [ORGANIZATION] laptop computers are considered part of the in-house environment and will be subjected to the same requirements as in-house workstations.

Anti-Virus Software

Anti-Virus checking software will be upgraded in a timely manner and:

1. Be installed on all the [ORGANIZATION] applicable computer systems;
2. Not be turned off or disabled; and
3. Be updated regularly according to the software vendor's specification.

Reporting Procedures

Viruses will be reported by the user to the Help Desk and the user's manager. When a virus is reported, managers will contact the Information Security Officer using the Incident Handling Form, Exhibit A.

Rationale

This policy formalizes roles, responsibilities, and mandated secured information-sharing relationships between business partners and the [ORGANIZATION]. This policy assures compliance with Federal and State laws that describes the procedures established and used by the [ORGANIZATION] for ensuring the integrity, confidentiality, and availability of the corporate information received. The policy also assures that the [ORGANIZATION] has the capability to deal with the growing threat of computer-based attacks in order to mitigate the risk of serious disruptions and damages to its critical infrastructure. Federal and State laws requires that security responsibility be assigned to a specific individuals or [ORGANIZATION], and that the assignment be documented. These responsibilities would include the management and supervision of:

- Use of security measures to protect data;
- Conduct of personnel in relation to the protection of data; and
- Procedures for ensuring the administrative, technical, and physical security of the corporate sensitive records.

This assignment is important to provide an organizational focus and importance to security, and to pinpoint responsibility. Additionally, the [ORGANIZATION] must comply with Federal, State, and local laws, rules and regulations to prevent loss of Federal tax information and support, and/or to avoid fines and penalties.

Risk

Failure to comply with this stated policy might put the [ORGANIZATION] in irreparable harm. Non-compliance with this policy and supporting policies pertinent to information security is

subject to management review and action in conformance with [ORGANIZATION] disciplinary policies, State, or Federal laws, regarding computer crime.

Impact

User

This policy shall impact all users that have access to sensitive information, provides the knowledge that such access is recorded, and holds the individual user accountable and responsible for any unauthorized access.

Data Owners

This policy ensures that Data Ownership and responsibilities are established for information processing systems, to include accountability, access rights, and special handling requirements.

Managers

This policy will provide guidance in management's oversight of the [ORGANIZATION]'s development, implementation, and evaluation of its Information Security Management Program.

Technology Infrastructure Team

Working with Application Managers and Data Owners to ensure that proper decisions are made concerning the levels of concern for confidentiality, integrity, and availability of the data, and the protection level for confidentiality of the system. Ensure that audit logs are maintained, reviewed, and archived on all network devices, firewalls, etc.

Application Development/Database Administrators

Ensures systems are operated, maintained, and disposed of in accordance with internal security policies and practices outlined. Ensures periodic reviews are conducted to ensure compliance with the certification and accreditation program.