

Security Policy

USER DATA PROTECTION

This is a copyrighted document

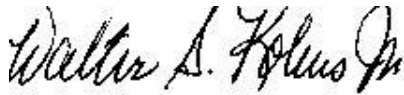
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your ORGANIZATION then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright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

INTRODUCTION	4
REFERENCES.....	4
<i>Regulatory.....</i>	<i>4</i>
<i>Security Standards</i>	<i>4</i>
PURPOSE.....	4
SCOPE.....	4
USE PROTECTION PROGRAM.....	5
POLICY	5
<i>User Data Protection.....</i>	<i>5</i>
<i>Data Integrity.....</i>	<i>5</i>
<i>Information Flow Control.....</i>	<i>5</i>
DATA ACCESS AUTHORITY TO PRODUCTION FILES	5
<i>Programmers and Analysts.....</i>	<i>6</i>
<i>Internal Audit/Operations Analysis.....</i>	<i>6</i>
<i>[ORGANIZATION] Information Security Group.....</i>	<i>6</i>
<i>System Software</i>	<i>6</i>
<i>Passwords Maintenance.....</i>	<i>6</i>
<i>Firewalls</i>	<i>7</i>
<i>Remote Desktop Security.....</i>	<i>8</i>
<i>Data Integrity Monitoring.....</i>	<i>8</i>
<i>Passive Detection of Physical Attack.....</i>	<i>8</i>
<i>System Boot Process</i>	<i>8</i>
RATIONALE	9
RISK	9
IMPACT	9
<i>Users</i>	<i>9</i>
<i>Data Owners</i>	<i>9</i>
<i>Managers</i>	<i>10</i>
<i>Application Development/Database Administrators.....</i>	<i>10</i>
<i>Help Desk.....</i>	<i>10</i>

Introduction

References

Regulatory

1. Insert regulatory requirements.

Security Standards

1. ISO 15408-2, Common Criteria, paragraph 6, Class FDP: User Data Protection.
2. ISO 15408-2, Common Criteria, paragraph 10, Class FPT: Protection of the TSF.
3. ISO 15408-2, Common Criteria, paragraph 12, Class TOE: Access TOE.
4. ISO 15408-2, Common Criteria, paragraph 13, Class FTP: Trusted Path/Channels.
5. International Standard, Information Technology – Code of Practice for Information Security Management, ISO/IEC 17799:2000(E), paragraph 9, Access Control.
6. DoD Directive 5200.28, Trusted Computer System Evaluation Criteria, C2 Class Assurance Level.

Purpose

The [ORGANIZATION] relies on information technology resources today to handle vast amounts of information. Because the information can vary widely in type and in degree of sensitivity, employees need to be able to exercise flexibility in handling and protecting the data. It would not be practical or cost effective to require that all data be handled in the same manner or be subject to the same protection requirements. Without some degree of standardization, however, inconsistencies can develop that could introduce risks.

Scope

The User Data Protection policy builds upon the Identification and Authentication Policy. The larger framework for the [ORGANIZATION]'s policy is based on the following three key principles:

1. Privacy. Encompasses the rights and desires of an individual to limit the disclosure of individual and corporate information;
2. Confidentiality. Recognizes that sensitive information may be released and shared for legitimate purposes, as long as adequate provisions are taken to protect the data. Confidentiality refers to the controlled conditions in which information is shared or released. These controlled conditions shall be illustrated in additional policies and procedures; and
3. Security. Consists of the control and processes (e.g. policies and procedures, design and implementation of technical measures) established to protect the [ORGANIZATION]'s sensitive information and systems. Such security measures not only are aimed at protecting privacy, but also ensuring the authentication, integrity, security, reliability, and availability of information systems.

Use Protection Program

Policy

User Data Protection

This policy applies to the [ORGANIZATION]'s information in the following formats with particular concern for protection of individual and corporate sensitive information:

1. Security. Protect individual and corporate sensitive information from loss, damage, inappropriate access, and unauthorized disclosure or use;
2. Integrity. Provide reasonable assurance that data, once entered, will not be subject to unauthorized modification, and that data will remain unaltered during transmission, storage, migration, and reuse;
3. Accountability. Monitor and record security-related events and link them to the originator; and
4. Technical Guidelines. Provide technical guidelines and collaborative solutions to respond to these requirements.

The [ORGANIZATION] computer and communications system's privileges of all users, systems, and programs shall be restricted based on the following principle of "least privileges":

1. Users shall be granted the "least privileges" required to accomplish their tasks;
2. Applications shall be granted the "least privileges" to perform their functions; and
3. General support systems shall be granted the "least privileges" to fulfill their role in a larger network.

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.

Information Flow Control

To ensure that proper information flow control is established, the use of data labeling shall be applied to sensitive data. All computer-resident information, which the information is classified as either sensitive or non-sensitive, shall have an operating system with discretionary access controls and auditing functionality to ensure the confidentiality, integrity, and availability of the system.

Data Access Authority to Production Files

Programmers and Analysts

Access by application programmers and analysts to production programs shall be limited through an approved change control request. This access shall be allowed for a specific timeframe to accomplish the approved change control request and then withdrawn. Programmers and analysts will not transform, alter, or modify the operating environment or standard operating procedures; programmers and analysts shall not make any modification that could have potential and/or significant impact on the stability and reliability of the infrastructure which impacts normal business operations.

Internal Audit/Operations Analysis

Internal auditors shall be authorized unrestricted read access for computer systems audits, provided management approves their request for audit privileges in advance. The request may be on the Internal Network Support-LAN Request Form or an approved substitute. The privileges authorized shall last for the duration of the audit. Requests for more than read or browse privileges during an audit must be documented and approved by management before privileges are granted.

Information Security Group

The security group shall be authorized unrestricted read access for computer systems, reviews or audits, provided the Information Security Officer approves their request for audit privileges in advance. The privileges authorized shall last for the duration of the review or audit.

System Software

Access authorizations shall be appropriately limited. Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators shall be specifically prohibited from accessing system software. The access capabilities of systems programmers shall be periodically reviewed to see that access permissions correspond with job duties. Justification and management approval for access to systems software shall be documented and retained.

Passwords Maintenance

Individuals assigned with maintaining User IDs shall only be given access to enter, change, delete, etc., user profiles and no other permissions or access to other files or system level programs.

Web Sites

There are many interdependencies among the security controls on the Web. The [ORGANIZATION]'s Web site shall provide the following minimum features and controls:

1. The site's domain naming service entries for all URL-referenced systems must be resolvable;
2. The site must maintain logging. Access to logs must be limited to authorized personnel. Logs must be retained in a secure but retrievable format, in adherence to legislative, regulatory and legal requirements;

3. The site must use a Federal standard encryption mechanism for sensitive data transmission commensurate with the level of protection required;
4. The site's pages that contain or accept sensitive data should be made non-cacheable. The site must inform users of all pages containing sensitive data that will be cached to local storage;
5. The site must meet physical security requirements, such as access-controlled area, roster of authorized personnel, suitable equipment, and emergency contact information;
6. The site must meet logical security requirements, such as secure password policies, Webmaster contact, Hyper Text Transfer Protocol Daemon server configured for least privilege, and separate development/production systems;
7. If the site has a transaction mechanism in place, the transaction must be documented and the server's private key protected by a strong passphrase. Sensitive information must be periodically removed from the Web server. The operating system platform must be documented and its integrity assured. Backups and restore capabilities must be in place;
8. The site shall not allow sensitive data to reside on a publicly accessible server without the written approval of the Information Security Officer;
9. The site shall not allow a publicly-accessible server, such as FTP, or Web, on the [ORGANIZATION] network;
10. The site shall store sensitive data on a controlled system, apart from the Web documents;
11. If possible, read-only data in the site shall be stored on unalterable media;
12. The site shall not allow Web development on production Web servers. Proper change control policies and procedures must be complied with; and
13. The site must not allow system access to internal resources, such as network file systems, printers, and accounts.

Firewalls

As a matter of the [ORGANIZATION]'s policy, all firewall services are denied, except those explicitly permitted and approved. Therefore, the procurement of a firewall product, installation of the product, and turning on the services of the firewall product must be coordinated and approved by the Information Security Officer. An examination and evaluation shall be required every quarter or when one of the following occurs:

1. A change or modification is made to the system software; and
2. There is a change in system administrators or Information Security Representative personnel.

Remote Desktop Security

The system administrator shall put into place security mechanisms that ensure all users take steps to protect the confidentiality, integrity, and availability of the [ORGANIZATION]'s information.

The system administrator shall deploy the necessary hardware and software to ensure that all such external access is identified, authenticated, tracked and logged. This means that the site is making a good-faith effort to ensure:

1. That the identity of all users is authenticated, and only properly validated users are granted access;
2. That a log is kept to permit, should the need arise, historical review of off site access to the [ORGANIZATION], by time, date, access port identity and user identity;
3. That the system administrator shall ensure all remote connections be protected anytime when the user leaves the system unattended. The system administrator shall enforce this access control by using a locking "screen saver," which locks user interaction after no more than five (5) minutes of inactivity.

Data Integrity Monitoring

All of the [ORGANIZATION]'s computer systems shall be monitored by an intrusion detection system that tracks the accessibility, movement, data transfer, and disposition of the data to alleviate any attempt to compromise the integrity, confidentiality or availability of a resource. The system shall provide feedback mechanisms, which informs the security staff as to the effectiveness of other components of the security system. The system shall also provide a trigger or gating mechanism that determines when to activate planned responses to an incident. The system administrator shall identify exploited vulnerabilities and react to security incidents. System administrators shall stay informed of all system advisories, flaws, and install software updates accordingly.

Passive Detection of Physical Attack

To ensure defense against passive line tapping, all of the [ORGANIZATION] users shall encrypt any sensitive information data being transmitted where a physical communication link is involved. All attacks shall be recorded via auditable means and reported as set forth in the [ORGANIZATION]'s incident reporting guidelines and procedures.

System Boot Process

Every computer within the [ORGANIZATION] that stores sensitive information shall follow approximately the same boot process. The system shall run a suite of self-tests during initial start-up, periodically during normal operation, at the request of the authorized user. The system administrator shall set security mechanisms that prevent the execution of a component if its integrity cannot be validated. The system administrator shall enforce automated recovery or manual recovery procedures to enter a maintenance mode where the ability to return to a secure state is provided.

Rationale

Within the [ORGANIZATION] network environment, the end users do not “own” the information for which they are allowed access. The [ORGANIZATION] is the actual “owner” of system objects on the network. This policy addresses the need for the implementation of a discretionary access control methodology. Discretionary Access Control methodology allows and promotes the central administration of the [ORGANIZATION]’s specific security policy. This policy covers all individuals responsible and accountable for the protection of sensitive information computer and communication devices, owned or operated, by [ORGANIZATION]. This policy assures that sensitive information is properly safeguarded, and 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.

Risk

Failure to comply with this stated policy may place 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 Agency disciplinary policies, and Federal laws, regarding computer crime. If user data protection solutions are not implemented, then the ability to analyze and trace the [ORGANIZATION] user actions will be severely limited and will not meet the legal requirements of Federal laws. Failure to meet this security requirement could cause loss of the [ORGANIZATION]’s information sharing with the Internal Revenue Service. If access control solutions are not implemented and configured properly, they can cause unauthorized browsing of sensitive information, which could cause employees, managers, and executives to be individually fined or terminated.

Impact

All areas of the [ORGANIZATION] shall comply with this User Data Protection policy; otherwise, an exception to the policy should be filed (and approved prior to implementation) if the policy requirement is not met. The following areas should comply with this policy:

Users

This policy shall impact all users that have access to the [ORGANIZATION] network or systems. This policy illustrates that all access is recorded and holds the individual user accountable and responsible for unauthorized access.

Data Owners

This policy shall assist the data owners in assuring that only authorized users have access to information data and that unauthorized access to information data will be determined and prevented when possible. This policy allows Data Owners to assign “least privileges” to sensitive information to ensure the confidentiality, integrity, and authorization of that information.

Managers

This policy shall allow management to take appropriate action to ensure that authentication is designed to combat fraud and make the [ORGANIZATION] network more secure. Management shall ensure that every program or system component will operate with the minimum set of privileges it needs to accomplish its task. Managers shall ensure that proper labeling of sensitive data is incorporated into identifying the [ORGANIZATION]'s system components.

Application Development/Database Administrators

This policy shall ensure that all administrators are responsible for implementing and monitoring approved access control solutions on computer systems. This policy shall ensure that all sensitive applications have the appropriate audit functions to abide by Federal laws, policies, and shall ensure that sensitive information flow is properly labeled and controlled within its own environment.

Help Desk

This policy shall ensure that continuity of access control solutions and data user protection solutions meet the needs of the Application Owners/Data Owners. The Help Desk will document any vulnerabilities identified in their ticket and report such findings to the system administrator for appropriate action.