

Security Policy

INFORMATION DATA OWNERSHIP

This is a copyrighted document.

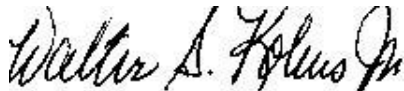
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your organization then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright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

1. Fill out the Clearance Document and sign it; and
2. 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:

1. 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.
2. Performance and Display Rights. RECIPIENT may not display any TESS Templates in public in any media format.
3. Exclusive or Nonexclusive. RECIPIENT has nonexclusive permission of the following Template(s) _____

 _____.
4. 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:
 - a. Mutual agreement of the parties to terminate the Agreement.
 - b. 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.
5. 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.
6. 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
 By: _____
 Walter S. Kobus Jr., VP
 Date: _____

Recipient
 By: _____
 Print Name: _____
 Date: _____

Table of Contents

INTRODUCTION	4
REFERENCE	4
<i>Regulatory</i>	4
<i>Security Standards</i>	4
PURPOSE.....	4
INFORMATION DATA OWNERSHIP PROGRAM.....	4
ROLES AND RESPONSIBILITIES OF DATA OWNERS	4
ROLES AND RESPONSIBILITIES OF CUSTODIANS	5
ROLES AND RESPONSIBILITIES OF USERS	5
DESIGNATING DATA OWNERS	ERROR! BOOKMARK NOT DEFINED.
DESIGNATING CUSTODIANS.....	6
DESIGNATING USERS.....	6
CHANGES IN STATUS	6
HANDLING OF INFORMATION FOLLOWING STATUS CHANGES.....	6
RISK	7
IMPACT	7
<i>Users</i>	7
<i>Data Owners</i>	7
<i>Managers</i>	7
<i>Application Development/Database Administrator's</i>	7
<i>Help Desk</i>	7

Introduction

Reference

Regulatory

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

Security Standards

1. ISO 15408, Common Criteria, paragraph 8, Class FMT: Security Management.
2. ISO 15408, Common Criteria, paragraph 9, Class FPR: Privacy.
3. ISO Standard 17799: Information Security Management Information Security.

Purpose

The purpose of this information data ownership policy is to provide policy for protecting information. This policy allows the [ORGANIZATION] Commissioner to delegate responsibilities and accountability for information to his senior managers. Information is no longer simply something, which supports the provision of a State service. Information itself has become a resource that must be protected on behalf of the corporation, client, customer, and other partnership that information is shared. The establishment of roles, responsibilities, and accountability are needed to properly manage and protect the information assets within the [ORGANIZATION]. To this end, this policy defines the roles of Data Owners commonly referenced as Data Owners or Executive Sponsors, Custodians, and Users. Information protection can no longer be a concern of information technology technical specialists and security professionals alone -- it must instead be addressed by a large team of individuals, each of which makes their own unique contribution.

Information Data ownership Program

Roles and Responsibilities of Data Owners

Data Owners are senior managers with the authority for acquiring, creating, and maintaining information systems within their assigned area of control. Data Owners are responsible for:

1. Categorizing the information for which they have been designated as a Data Owner using classifications defined in the Data Classification Policy;
2. Authorizing User access to information based on the need-to-know;
3. Defining the validation rules used to verify the correctness and acceptability of input data;
4. Insuring a sufficient level of training takes place for people entering or modifying data in the system;
5. Assisting in contingency planning efforts by identifying their information sensitivity and criticality on their specific application support systems;

6. Making decisions about the permissible uses of information;
7. Understanding the uses and risks associated with the information for which Data Owners are accountable. This means that Data Owners are responsible for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security related control deficiencies pertaining to the information for which they are designated as the Data Owner; and
8. When a system has more than one Data Owner's information residing on the system or commingled, the Data Owner's must ensure that the system shall meet the highest level of security of the information needing protection.

Roles and Responsibilities Of Custodians

Information Custodians are individuals (often staff within the Information Systems Division or division systems administrators) in physical or logical possession of information from Data Owners. Custodians are responsible for:

1. Protecting the information in their possession from unauthorized access, alteration, destruction, or usage;
2. Providing and administering general controls such as back-up and recovery systems consistent with company policies and standards;
3. Establishing, monitoring and operating information systems in a manner consistent with policies and standards;
4. Providing Data Owners with reports about the resources consumed on their behalf (often via a charge-back system), as well as reports indicating User activities; and
5. Changing the production information in their possession only after receiving explicit and temporary permission from the Data Owner.

Roles and Responsibilities Of Users

Information Users are individuals who have been granted explicit authorization to access, modify, delete, and/or utilize information by the relevant Data Owner. Users must:

1. Use the information only for the purposes specifically approved by the Data Owner;
2. Comply with all security measures defined by the Data Owner, implemented by the Custodian, and/or defined by policies and standards;
3. Refrain from disclosing information in their possession (unless it has been designated as Public) without first obtaining permission from the Data Owner; and
4. Report all situations where they believe an information security vulnerability or violation may exist.

Local management must also provide Users with sufficient time to receive periodic information security training. Users of personal computers have special responsibilities for example relating to back up and virus screening.

If there is several potential information Data Owners, higher-level management must assign Data Ownership responsibility to the senior manager of the business unit, which makes the greatest use of the information. When acting in their capacity as a Data Owner, this individual must take into consideration the needs and interests of other stakeholders which rely upon or have an interest in the information. With the exception of operational and network information, managers in the Information Systems Division must not be a Data Owner for any information. A Data Owner's roles and responsibilities may be delegated to any manager in the Data Owner's business unit. A Data Owner's roles and responsibilities may not be assigned or delegated to contractors, consultants, or individuals in outsourcing firms or external service bureaus.

Designating Custodians

Management must specifically assign responsibility for the control measures protecting every major production type of information. Data Owners are responsible for identifying all those individuals who are in possession of the information for which they are the responsible party. These individuals by default become Custodians. Although special care must be taken to clearly specify security-related roles and responsibilities when outsiders are involved, it is permissible for Custodians to be contractors, consultants, or individuals at outsourcing firms or external service bureaus.

Designating Users

Users may be employees, temporaries, contractors, consultants, or third parties with whom special arrangements (such as nondisclosure agreements) have been completed. All Users must be known to and authorized by Data Owners. The security-relevant activities of all Users must be tracked and logged by Custodians. To allow proper privilege assignment and activity logging, Users must always be specific individuals; Users must not be defined as departments, project teams, or other groups.

Changes In Status

Due to promotions, transfers, retirements, etc., the individuals who play the roles of information Data Owners, Custodians, and Users will change on a regular basis. It is the responsibility of the local manager of all individuals to promptly report status changes. Custodians must maintain access control systems so that previously provided User privileges are no longer provided whenever there has been a User status change. When a Custodian has a change in status, it is the responsibility of the Data Owner to promptly assign a new Custodian.

Handling Of Information Following Status Changes

Users who change their status must leave all production information with their immediate manager. Soon after a User has a change of status, both computer-resident files and paper files must be reviewed by the User's immediate manager to determine who should be given possession of the files, and/or the appropriate methods to be used for file disposal or destruction. The manager must then promptly reassign the User's duties as well as specifically delegate responsibility for information formerly in the User's possession.

Information security can no longer be a concern of technical specialists alone -- a large team of individuals, each of which makes their own unique contribution, must instead address it.

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 Agency disciplinary policies, State, or Federal laws, regarding computer crime. If access control solutions capabilities are not provided, then the ability to analyze and trace [ORGANIZATION] user actions will be severely limited and not meet the legal requirements of both Federal and State laws. If access control solutions are not implemented and configured properly, they can cause unauthorized browsing of corporate data, which could cause employees, managers, and executives to be individually fined or dismissed.

Impact

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

Users

This policy shall impact all users that have access to the [ORGANIZATION] network or systems. This policy illustrates that any access is recorded and holds the individual user accountable and responsible for unauthorized access. This policy also ensures that sensitive information flow is controlled in its unique environment.

Data Owners

This policy illustrates the background, framework, and understanding that will enable Data Owners to embrace the philosophy of information data ownership and commit to its principles ensuring its confidentiality, integrity, and authorization.

Managers

This policy will allow management to address the fundamental attributes of data ownership to include: responsibility, long-term effectiveness and adaptability.

Application Development/Database Administrator's

This policy illustrates the methodology that will enable Application Development/Database Administrator's to integrate the practice of information data ownership into the management of their respective areas of concern. Ensure that all sensitive applications have the appropriate audit functions to abide by Federal laws, State laws, and policies. Ensure that sensitive information flow is properly labeled and controlled within its own environment.

Help Desk

This policy identifies the information ownership necessary to respond to customer needs.

