

Security Policy

DATA CLASSIFICATION

This is a copyrighted document

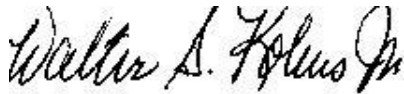
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your organization then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright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

Recipient

By: _____

By: _____

Walter S. Kobus Jr., VP

Print Name: _____

Date: _____

Date: _____

Table of Contents

INTRODUCTION	4
REFERENCE	4
<i>Regulatory.....</i>	<i>4</i>
<i>Security Standards</i>	<i>4</i>
PURPOSE.....	4
DATA CLASSIFICATION PROGRAM.....	4
POLICY	4
<i>Applicable Information</i>	<i>4</i>
<i>Consistent Protection</i>	<i>4</i>
CLASSIFICATION LABELS.....	5
<i>Sensitive Information</i>	<i>5</i>
<i>Non-Sensitive Information</i>	<i>5</i>
DATA CLASSIFICATION MATRIX.....	5
QUESTIONS CONCERNING DATA CLASSIFICATION.....	5
CLASSIFIED INFORMATION (NATIONAL/HOMELAND SECURITY)	6
SENSITIVE APPLICATIONS.....	6
<i>Restricted Application.....</i>	<i>6</i>
<i>Critical Applications</i>	<i>6</i>
RATIONALE	6
RISK	6
IMPACT	7
<i>Users.....</i>	<i>7</i>
<i>Data Owners.....</i>	<i>7</i>
<i>Managers</i>	<i>7</i>
<i>Application Development and Database Administrators</i>	<i>7</i>
<i>Information Security Officer</i>	<i>7</i>

Introduction

Reference

Regulatory

1. Sarbanes-Oxley Act
2. Health Insurance Portability and Accountability Act.
3. Gramm-Leach-Bliley Act.

Security Standards

1. International Standard, Information Technology – Code of Practice for Information Security Management, ISO/IEC 17799:2000(E),
2. ISO 15408, Common Criteria, paragraph 8, Class FMT, Security Management.
3. ISO 15408, Common Criteria, paragraph 9, Class FPR, Privacy.

Purpose

The purpose of this data classification policy is to provide a system for protecting information that is critical and sensitive to the [ORGANIZATION]. All users who may come into contact with sensitive information are expected to familiarize themselves with this data classification policy and to consistently use it.

Data Classification Program

Policy

The [ORGANIZATION] data classification system has been designed to support the “need-to-know”, so that information will be protected from unauthorized disclosure, use, modification, and deletion. Consistent use of this data classification system will facilitate business activities and help keep the costs for information security to a minimum. Without the consistent use of this data classification system, the [ORGANIZATION] risks loss of client confidence, internal operational disruption, and excessive costs.

Applicable Information

This data classification policy is applicable to all information in the [ORGANIZATION]’s possession. For example, client records, employee records, sensitive information from suppliers, business partners and others must be protected with this data classification policy. No distinctions between the word data, information, knowledge, and wisdom are made for purposes of this policy.

Consistent Protection

Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity; regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose(s) it serves. Although this document provides overall policy to achieve consistent

information protection, users shall be expected to apply and extend these concepts to fit the needs of day-to-day operations.

Classification Labels

Sensitive Information

Information identified by the [ORGANIZATION] as critical and/or restricted is defined as follows:

1. *Critical Information:* Information that must be available for the [ORGANIZATION] to effectively perform its mission and meet legally assigned responsibilities, and for which special precautions are taken to ensure its accuracy, relevance, timeliness, and completeness. This information, if lost, could cause significant financial loss, inconvenience, or delay in performance of the [ORGANIZATION]'s mission.
2. *Restricted Information:* Information that has limitations placed upon both its access within and disclosure outside the [ORGANIZATION]. Consistent with both State and Federal Privacy Laws, this information falls into two categories:
 - a. *Restricted Mandatory.* Information that has limitations upon its internal access and that may be disclosed only in accordance with an executive order, public law, or other Federal Statute and supporting the [ORGANIZATION]'s policies.
 - b. *Restricted-Discretionary.* Information that has limitations upon its internal access and that may be withheld from external disclosure solely in accordance with the [ORGANIZATION]'s policies consistent with the *Open Records Act*.

Non-Sensitive Information

Non-sensitive information can be classified into two types:

1. *Controlled:* Non-sensitive information that management has determined to require limitations or internal access/distribution on a need to know basis; does not include restricted information.
2. *Non-controlled:* Information that can be made available to anyone without exception.

Data Classification Matrix

Refer to *Appendix A: Classification Matrix* for the handling and security requirements for information based on its classification.

Questions Concerning Data Classification

Questions concerning information classification should be directed to the Information Security/Privacy Officer.

Classified Information (National/Homeland Security)

Information about national or homeland defense and foreign relations of the United States that has been determined under Executive Order 12356 to require protection against unauthorized disclosure and has been so designated.

Sensitive Applications

Restricted Application

A computer application that requires protection because the information or process is classified as restricted, that is, has limitations placed upon both its internal access and external disclosure.

Critical Applications

A computer application that requires protection because the process is critical to the operation of the [ORGANIZATION], that is, if adversely manipulated or not run on or near schedule will cause significant financial loss to the Agency in financial loss (interest revenue), inconvenience, or delay in performance of the [ORGANIZATION] mission.

Rationale

It is essential that the [ORGANIZATION]'s sensitive data be protected. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. An appropriate level of security (protection) should be established for each data classification. All information resources should be categorized and protected according to the requirements set for each classification, and the data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the [ORGANIZATION]. This policy covers all individuals responsible and accountable for the protection of sensitive information computer owned or operated, by the [ORGANIZATION]. This policy assures financial and corporate 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 might place the [ORGANIZATION] in irreparable harm. Non-compliance with this policy and supporting policies pertinent to information security regarding computer crime is subject to management review and action in conformance with Agency disciplinary policies, State or Federal laws. If data classification procedures are not provided, then the ability to protect information will be severely limited and will not meet the legal requirements of both Federal and State 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 financial or 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

The individuals entrusted with the data are responsible for protecting the data consistent with the security requirements defined by the data custodian.

Data Owners

Data custodians have the responsibility for classifying data on the [ORGANIZATION] network.

Managers

This policy shall allow management to take appropriate action to ensure that all users are aware of the actions pertaining to safeguarding sensitive information in the [ORGANIZATION].

Application Development and Database Administrators

These administrators are responsible for implementing and monitoring approved access control solutions to ensure that all sensitive applications have the appropriate audit functions to abide by Federal and State laws, and policies.

Information Security Officer

The security team needs to ensure that continuity of access control solutions meet the needs of Application Owners/Data Owners to safeguard sensitive information.