

SECURITY POLICY

Cryptography

THIS IS A COPYRIGHTED DOCUMENT

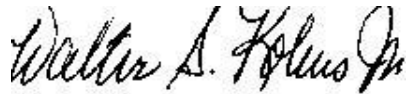
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your ORGANIZATION then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright 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>	4
<i>Security Standards</i>	4
PURPOSE.....	4
SCOPE.....	4
CRYPTOGRAPHY PROGRAM.....	5
POLICY	5
<i>Hardware vs. Software Implementations</i>	5
<i>Electronic Storage Media</i>	5
<i>Server, Workstation, and Laptop Encryption</i>	5
<i>Remote Access</i>	5
<i>Smart Cards</i>	5
<i>Back-up Storage Media and Supervisor Password</i>	5
<i>E-mail Encryption</i>	6
<i>Non-repudiation Services</i>	6
<i>Encryption of Passwords</i>	6
<i>Key Management, Key Escrow, and Key Recovery</i>	6
<i>Information Security Officer</i>	6
RATIONALE	6
RISK	7
IMPACT	7
<i>Users</i>	7
<i>Data Owners</i>	7
<i>Managers</i>	7
<i>Infrastructure Group</i>	7
<i>Application Development/Database Administrators</i>	7
<i>Help Desk</i>	7

Introduction

References

Regulatory

1. Insert regulatory requirements.

Security Standards

1. Sarbanes-Oxley Act
2. ISO 15408-2, Common Criteria, paragraph 5, Class FCS: Cryptographic Support.
3. ISO 15408-2, Common Criteria, paragraph 13, Class FTP: Trusted Path/Channels.
4. Information Technology – Code of Practice for Information Security Management, ISO/ECI 17799.
5. DoD Directive 5200.28, Trusted Computer System Evaluation Criteria, C2 Class Assurance Level.
6. FIPS PUB 140-2, Security Requirements For Cryptographic Modules.
7. FIPS PUB 46-3, Data Encryption Standard.
8. FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard.
9. FIPS PUB 81, DES Modes of Operation.
10. FIPS PUB 113, Computer Data Authentication.
11. FIPS PUB 171, Key Management Using ANSI X9.17.
12. FIPS PUB 180-1, Secure Hash Standard.
13. FIPS PUB 186-2, Digital Signature Standard.
14. NIST Special Publication 800-2, Public Key Cryptography.
15. NIST Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption.
16. NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government.
17. Algorithm (TMOVS): Requirements and Procedures

Purpose

The purpose of this policy is to illustrate that the value of the [ORGANIZATION] information lies in its availability, but to safeguard information it must be made inaccessible to all except those who are duly authorized. The [ORGANIZATION] depends upon information technology (IT) systems to perform essential and mission-critical functions. In the current environment of increasingly open and interconnected systems and networks, network and data information security are essential for the optimum use of this information technology. The purpose of this policy describes cryptography as a tool for satisfying a wide spectrum of the [ORGANIZATION] Information Security Management Program needs and requirements.

Scope

Emerging computer and communications technologies are radically altering the ways in which the [ORGANIZATION] communicates and exchanges information. The [ORGANIZATION] networks store and exchange an ever-increasing amount of highly sensitive information,

including individual taxpayer and corporate taxpayer data requiring protection appropriate to their value. In this electronic environment, the need for privacy-enhancing technologies is apparent. Through the use of cryptography, information stored and transmitted by the [ORGANIZATION] computers shall be protected against interception.

Cryptography Program

Policy

This policy addresses the [ORGANIZATION] cryptographic techniques used for the protection of information that is considered at risk.

Hardware vs. Software Implementations

Cryptography shall be implemented in either hardware or software when applicable. The Information Security Officer, prior to use, must approve all encryption products, processes, and standards. The Information Security Officer shall maintain a list of approved encryption algorithms and acceptable key lengths for each algorithm.

Electronic Storage Media

Sensitive information shall be protected against unauthorized disclosure when it is stored on electronic storage media if the information cannot be protected using sufficient physical or logical controls, and the information is at risk of being compromised or stolen.

Server, Workstation, and Laptop Encryption

If a server, workstation, or laptop contains sensitive information, then that data shall be encrypted if the information cannot be protected using sufficient physical or logical controls, and the information is at risk of being compromised or stolen.

Remote Access

Accessing databases, containing sensitive Information from a remote location (i.e., a location not directly connected to the Local Area Network) will require adequate encryption safeguards to prevent unauthorized entry.

Smart Cards

Smart cards shall have both identification and authentications features and provide data encryption as well.

Back-up Storage Media and Supervisor Password

Any data sent off-site for storage should be afforded the same level of security as the on-line data. To protect from unauthorized disclosure, modification, or loss, the entire electronic storage media should be encrypted along with supervisor password before sending off-site. All backup media shall be stored in a fire resistant container. The access privilege to backup and restore files and directories shall be limited to authorize personnel only.

E-mail Encryption

If any sensitive information is transmitted via email, then the use of encryption is mandatory. The information can be stored in a separate file, protected accordingly using encryption, and then attached to the email. Users may not encrypt any emails without an encryption program approved by the Information Security Officer.

Non-repudiation Services

User authentication or identification must be coupled with the encryption and data transmission processes to be certain that sensitive information is delivered only to authorized parties.

Encryption of Passwords

To prevent passwords from being disclosed to sniffer attacks, passwords must always be encrypted when held in storage or when transmitted over communications systems. The password management system shall store passwords in encrypted form using a one-way encryption algorithm. Supervisor passwords shall be encrypted and stored off-site with backup files each time the password is changed to ensure for a complete recovery.

Key Management, Key Escrow, and Key Recovery

The Information Security Officer will ensure that an approved key management system is in place for the secure administration and distribution of cryptographic keys throughout their entire key life cycle. All keys will be generated through an approved encryption package and securely stored for the unlikely event of key loss due to unexpected circumstances.

Information Security Officer

The success of implementing encryption practices depends on the crucial role performed by the Information Security Officer. It is important that the Information Security Officer approve encryption products, and set standards for use. This is especially critical for standards such as the minimum length of encryption keys, key recovery, and selection of encryption software.

Rationale

Encryption provides one of the few ways to safeguard logon scripts, taxpayer information, corporate taxpayer information, passwords, certificates used to access the enterprise network, encryption keys, pseudo-random number generator seeds, and other security parameters. Without encryption, these quantities may be inadvertently disclosed to persons who have access to telecommunication system buffers, temporary working memory inside a computer, etc.

This policy assures taxpayers 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. The implementation of cryptographic security controls is important to provide a [ORGANIZATION] focus towards the importance of security, and to pinpoint responsibility. Additionally, this policy ensures that the [ORGANIZATION] is within compliance with Federal, State, and local laws, rules and regulations to prevent loss of Federal tax information and corporate taxpayer data.

Risk

Failure to comply with this stated policy may 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 encryption processes are not implemented and configured properly, they can cause system performance degradation or operational hurdles for the user. In addition, improperly configured encryption processes can give the [ORGANIZATION] a false sense of security; thinking that the confidentiality of sensitive information is protected through encryption, when in fact it is not.

Impact

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

Users

The users of information are responsible for letting the Responsible party/Application Owners know what their needs are for the protection of the [ORGANIZATION] sensitive information, especially for its integrity and availability. Users shall use a file encryption tool approved by the Information Security Officer to safeguard sensitive information.

Data Owners

Ensure that cryptographic security solutions are established for each data system where applicable.

Managers

Managers are responsible for ensuring that adequate cryptographic solutions are applied within their programs and that they are tested, in compliance with Federal standards.

Infrastructure Group

Working with Application Managers and Data Owners ensure that proper cryptographic solutions are made concerning the confidentiality, integrity, and availability of the data.

Application Development/Database Administrators

Responsible for implementing and monitoring cryptographic solutions on computer systems. Need to ensure that continuity of cryptographic services meet the needs of Application Owners/Data Owners, as well as analyzing technical vulnerabilities in the system regarding security implications.

Help Desk

In regards to any cryptographic problems refer caller to the Information Security Officer.