

SECURITY POLICY

COMMUNICATION

This is a copyrighted document

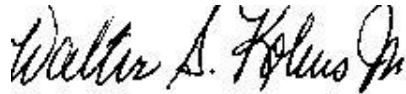
If you decide that you want to download this document and use it "as is" or make an adaptation (called Derivative Works) of the Template for use in your ORGANIZATION then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright 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
By: _____
Walter S. Kobus Jr., VP
Date: _____

Recipient
By: _____
Print Name: _____
Date: _____

TABLE OF CONTENTS

INTRODUCTION	4
REFERENCES.....	4
<i>Regulatory</i>	4
<i>Security Standards</i>	4
PURPOSE.....	4
SCOPE.....	4
COMMUNICATIONS PROGRAM	4
POLICY	4
<i>Communications Equipment</i>	4
<i>Transmission Lines</i>	5
<i>Telecommunications Equipment</i>	5
<i>Communications Network</i>	5
VIRTUAL PRIVATE NETWORKS	5
CONTRACTING SITES COMMUNICATIONS	5
INTERNAL/EXTERNAL DESKTOP MODEMS.....	6
DIAL-IN AND DIAL-OUT COMMUNICATIONS	6
FACSIMILE MACHINES (FAX).....	6
CABLING SECURITY	6
OTHER FORMS OF INFORMATION EXCHANGE	7
CLOCK SYNCHRONIZATION.....	7
RATIONALE	7
RISK	7
IMPACT	7
<i>Users</i>	7
<i>Data Owners</i>	7
<i>Managers</i>	8
<i>Infrastructure Group</i>	8
<i>Application Development/Database Administrator's</i>	8
<i>Help Desk</i>	8

Introduction

References

Regulatory

Insert regulatory requirements

Security Standards

1. ISO 15408-2, Common Criteria, paragraph 4, Class FCO: Communication.
2. ISO 15408-2, Common Criteria, paragraph 13, Class FTP: Trusted path/channels.
3. Information Technology – Code of Practice for Information Security Management, ISO/ECI 17799
4. DoD Directive 5200.28, Trusted Computer System Evaluation Criteria, C2 Class Assurance Level

Purpose

To establish the [ORGANIZATION]'s Policy for the confidentiality, integrity, and availability of the [ORGANIZATION] information assets transmitted over a communications network, using communications or network controls.

Scope

Information security is an area of pivotal concern and importance to the [ORGANIZATION] in regards to its computers and communication networks. Given the rapid pace of technological change, the decentralization of computing, and the proliferation of computers, networks and users of varying capabilities in the [ORGANIZATION] setting, it is essential that these systems be protected from misuse and unauthorized access.

Communications Program

Policy

Management will take appropriate action to ensure that all employees are aware of the security measures taken when transmitting the [ORGANIZATION] information assets across a communications network. Management will initiate or direct the development of processes, procedures, and standards, in accordance with the [ORGANIZATION] guidelines, which would corroborate that the data has not been altered or destroyed while being transmitted.

Communications Equipment

All communications equipment including computer systems, and network devices are owned by the [ORGANIZATION] and are to be used for the [ORGANIZATION]'s related activities only. The Information Security Officer shall approve any personally owned equipment brought into the [ORGANIZATION] environment.

Transmission Lines

The data paths associated with on-line processing shall be kept as error-free and secure as possible. This is of vital concern when sensitive data is being transmitted. Managers shall evaluate the data that is being processed and use appropriate techniques.

Telecommunications Equipment

All telecommunications equipment, such as routers, PBX systems, multiplexors, and modems shall be protected. Security features in telecommunications equipment shall be used to protect these telecommunications assets. If the equipment uses default passwords, the passwords must change if this is technically feasible.

Communications Network

Sensitive information must be encrypted before transmitting over a communications network when:

1. Using an external public communications network, the information is considered too sensitive for the general public to read or when using the internal communications network, the information is considered too sensitive for a general computer user to read;
2. Remote administration of hardware, software, or applications is performed; and
3. Third party network connections to network devices (i.e., hosts, routers) are needed.

Virtual Private Networks

A Virtual Private Network must allow for encryption that is accordance with [ORGANIZATION]'s Cryptography Policy, strong Identification by user or machine, and non-repudiation when required.

Contracting Sites Communications

A contractor site that require connectivity to the [ORGANIZATION] network shall comply with the [ORGANIZATION]'s Security Policies and Procedures. The contracting officer and or contracting officer's representative must ensure that the following contract requirements are specified within the statement of work:

1. All contract personnel must have appropriate contractor screening;
2. The contractor must comply with all security policies and procedures; and
3. The Internal Audit Department or the Information Security Officer shall be allow to visit the contractor site to conduct audits and reviews.

No connectivity shall be made between the contractor's computer resources and the [ORGANIZATION]'s furnished computer equipment, local area network or wide-area network,

or the [ORGANIZATION]'s Intranet, without prior review by and written consent of the Information Security Officer.

Internal/External Desktop Modems

Individual desktop internal/external modems in the [ORGANIZATION] network LAN environment are not authorized for use. Exceptions for such connection shall be made only if approved by the Technology Infrastructure Manager and authorized access control systems have been installed and approved by the Information Security Officer.

Dial-In and Dial-Out Communications

Authorized users shall be provided with the following dial-in and dial-out communications:

1. Dial-in to the authorized user's server to extract and or update email files while away from his duty office;
2. Dial-in to access the [ORGANIZATION] gateways away from the user's workstation; and
3. Dial-out to access other customer facilities or authorized services.

Facsimile Machines (Fax)

The telecommunication lines used to send fax transmissions are not secure. To reduce the threat of intrusion observe the following:

1. Have a trusted staff member at both the sending and receiving fax machines or have a locked room for the fax machine with custodial coverage over outgoing and incoming transmissions;
2. Accurately maintain broadcast lists and other preset numbers of frequent recipients of Federal tax information. Place fax machines in a secured area; and
3. Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes:
 - a) a notification of the sensitivity of the data and the need for protection; and
 - b) a notice to unintended recipients to telephone the sender - collect if necessary - to report the disclosure and confirm destruction of the information.

Cabling Security

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

Other Forms of Information Exchange

Procedures and controls shall be in place to protect the exchange of information through the use of voice and video communications facilities.

Clock synchronization

Where a computer or communications device has the capability to operate a real-time clock, it shall be set to an agreed standard, e.g., Universal Coordinated Time (UCT) or local standard time. As some clocks are known to drift with time, there shall be a procedure that checks for and corrects any significant variation.

Rationale

This policy assures that the [ORGANIZATION] has the capability to deal with the growing threat of computer-based communication attacks in order to mitigate the risk of serious disruptions and damages to its critical infrastructure. The implementation of communication security controls is important to provide the [ORGANIZATION]'s 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 data.

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 is subject to management review and action in conformance with Agency disciplinary policies, State, or Federal laws, regarding computer crime. If communications security controls are not implemented and configured properly, they can cause system performance degradation or operational hurdles for the user.

Impact

All areas of the [ORGANIZATION] shall comply with this communication 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]'s sensitive information transmitted over the communications network.

Data Owners

Data owners ensure that communication security controls are established for each data system where applicable.

Managers

This policy will provide guidance in management's oversight of the [ORGANIZATION]'s Information Security Management Program. Division Director's will ensure that adequate communication controls are applied within the program.

Infrastructure Group

Working with Application Managers and Data Owners, the Infrastructure Group ensures that proper communications controls are made regarding the levels of concern for confidentiality, integrity, and availability of the data, and the protection level for confidentiality of the system.

Application Development/Database Administrator's

These Administrators are responsible for implementing and monitoring approved communications solutions on computer systems. Administrators will ensure that continuity of communication services meet the needs of Application Owners/Data Owners and analyze technical vulnerabilities in the system regarding security implications.

Help Desk

In regards to major communication problems refer caller to the Information Security Officer.