

Security Policy

PHYSICAL SECURITY

This is a copyrighted document

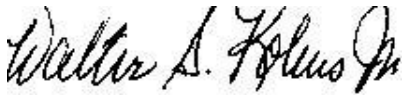
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your ORGANIZATION then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright 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
<i>General</i>	4
<i>Policy</i>	4
RESPONSIBILITIES	4
<i>Manager Computer Facility</i>	4
<i>Workstations, Terminals, and Laptops (Access Units)</i>	5
<i>Building Facility Manager</i>	5
ACCESS PROCEDURES	5
<i>Secure Working Areas</i>	6
<i>Enforcement</i>	6
<i>Other Areas</i>	6
<i>Preventive Measures</i>	6
ACCESS CONTROL LIST.....	6
<i>Establishment</i>	6
POSTING AND DISPOSITION	6
IDENTIFICATION BADGES	7
<i>Requirements</i>	7
<i>Lost or Stolen Badges</i>	7
<i>Forgotten Badges</i>	7
<i>Verification</i>	7

Introduction

General

A balanced security program must include a solid physical security foundation. A solid physical security foundation protects and preserves information, physical assets, and human assets by reducing the exposure to various physical threats that can produce a disruption or denial of computer service.

Policy

Managers are responsible for ensuring that corporate information assets under their control are properly protected through the implementation of cost-effective physical security measures.

Responsibilities

Manager Computer Facility

The manager in charge of a computer facility that operates any platform computer system is responsible for providing adequate physical protection of computer equipment and data media. The manager will consider the following as a minimum:

- Ensure control access to the facilities and computers if required.
- Put computers behind doors that can be locked when unattended.
- Do not assume that physical access to the machine is enough security. Require locked cabinets.
- Place computer and associated I/O hardware in locked cabinets as possible.
- Make sure your machine has some sort of power conditioning, such as an Uninterruptible Power Supply (UPS). Make sure that the UPS or surge protector is designed to handle the amount of power that is needed in the facility.
- Ensure that an electrical line filter-to-filter voltage spikes.
- Use anti-static carpeting.
- Wear grounding wrist straps when opening up computers.
- Control the climate and environment of the computer.
- Make sure that the computer is not in a room where it will overheat. Make sure that there is sufficient airflow to all parts of the computer to allow circulation of air. Temperature should be generally 50-80 degrees Fahrenheit (10-26 degrees Celsius).
- Install heating and cooling systems with air filters to protect against dust.
- Make sure that there is an adequate automated fire suppression system.
- Make sure staff is trained in the use of all fire suppression systems.
- Install smoke detectors near machines.
- Provide that ability to control humidity between 20% and 80%.
- Do not allow food or drink consumed near computers.
- Store all on-site backups in a secure location until rotate to off-site storage.
- Store backup tapes away from large metal objects to avoid damage from magnetic fields causes in lightning strikes.

- Don't put your computers behind glass walls where people can watch passwords being typed in.
- If you have raised floors or dropped ceilings make sure that walls extend to the ceilings and floors so that they cannot just be climbed over.
- Install a monitoring system that monitors the physical environment and warns you of and dangerous changes.

Workstations, Terminals, and Laptops (Access Units)

All the [ORGANIZATION] users are responsible for securing their access unit from unauthorized use.

- *Unattended During the Day:* Whenever a user is away from his or her access unit during the day, he or she must protect the [ORGANIZATION] information assets by either logging off of the computer, or activating a password protected screen saver.
- *Before Leaving the Work site:* At the end of the workday, each user is required to log off of his or her access unit. If a job must be run unattended after work hours, precautions must be taken to protect the access unit from unauthorized use.
- *Public Use Units:* Divisions and offices that provide access units for public use are responsible for ensuring that these access units are logged off when unattended, and at the end of each workday.
- *Technical Support Access:* The user must provide access for technical support staff to install upgrades and improvements to each access unit upon request.

Building Facility Manager

The Facilities Manager is responsible for evaluating the need for overall building security and for conducting periodic audits, reviews, or surveys of computer sites. It provides technical guidance on such matters as access control systems, use of the [ORGANIZATION] security force, personnel security, and physical security needs.

Access Procedures

At large centralized computer sites, control areas must be designated that effectively restrict and limit access to sensitive resources and specialized job input/output, such as checks, money orders, etc., and special terminals or input devices. Control areas should include computer rooms, tape libraries, telecommunications rooms, computer supply rooms, documentation libraries, production control, disbursement offices, operating system software support areas, special authorization terminal areas, personal computer work areas, production job output staging areas, terminal work rooms, building access areas, security officers' restricted areas, and other designated areas deemed restricted in nature.

Secure Working Areas

The construction of, and the physical security protection for, a secure working such as computer rooms, sensitive material storage, security offices, etc., must provide for the detection of forced or surreptitious entry of the facility, including those areas above false ceilings. Perimeter walls, floors, and ceilings may be constructed without regard to the thickness or type of material so long as they will show evidence of attempted forced entry and provide sound attenuation of STC 45 or better. However, if there is a possibility of surreptitious entry, alarms and or barriers must be used to prevent such entry.

Enforcement

The manager responsible for a controlled area may have unauthorized persons removed from the area. Assistance from the Building Service Security Force may be requested if available. The following exceptions apply:

1. Persons whose names are not on the access control list may be admitted to a control area at the discretion of the manager of that area. Their activities must be monitored while in the area.
2. Visitors may be admitted to a control area if they have received proper authorization. Visitors may also be required to have an escort at all times.
3. Information Security personnel will be admitted to a secured area upon presentation of official identification and can stay unescorted, in the secured area.

Building Facilities

[ORGANIZATION] offices and building shall have normal physical security controls in place. As a minimum the building shall be secure and restrict access to authorized personnel. Card access and monitoring devices shall be used to ensure that sensitive information is not comprised and access to control office work areas is monitored. Building facility manager will ensure that appropriate monitoring devices allow monitoring of primary accesses and that individuals are screened for access.

Preventive Measures

Areas should be designed having limited accessibility with personnel access controlled by a cipher lock system, card key system, or other physical access control methods.

Access Control List

Establishment

A control area is a work area to which access must be restricted because of the sensitive resources and equipment located there. Each control area shall establish an access control list of people who are authorized access to specific control areas. Managers of the control areas shall provide additions, deletions, or changes to the lists. Either the facility manager or designee, the ISR, shall maintain the access control list.

Posting and Disposition

The access control list pertaining to a specific area shall be posted on or near the doors of that area in such a manner that unauthorized personnel without detection cannot alter it.

Identification Badges

Requirements

Persons authorized access to control areas must be identified by a badge conspicuously displayed on their person above the waist. The use of a badge not issued to the bearer or any attempt to alter the badge warrants disciplinary action.

Lost or Stolen Badges

Employees must report lost or stolen badges immediately to the issuer of the badge. Security access systems supporting lost or stolen badges must immediately cancel previous access privileges until the lost or stolen badge is recovered and returned to the issuer.

Forgotten Badges

Temporary badges will be controlled and issued by the manager of the organization or designee to authorized personnel arriving without their assigned badges during normal duty hours. Authorized personnel arriving without badges at other than normal duty hours must report to the supervisor in charge of the facility or designee for issuance of a temporary badge.

Verification

The organization manager or designee must make an unannounced verification of badges at least annually to ensure authenticity and to correct any badge discrepancies.