

Security Policy

RESOURCE UTILIZATION

This is a copyrighted document

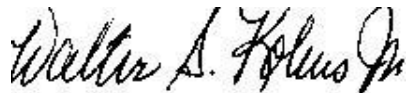
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your ORGANIZATION then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright 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
RESOURCE UTILIZATION PROGRAM	4
FAULT TOLERANCE	4
PRIORITY OF SERVICES	4
RESOURCE ALLOCATION	5
RESOURCE UTILIZATION.....	5
<i>Equipment Siting and Protection</i>	5
<i>Power Supplies</i>	6
<i>Cabling Security</i>	6
<i>Equipment Maintenance</i>	7
<i>Security of Equipment Off-Premises</i>	7
<i>Secure Disposal or Re-use of Equipment</i>	8
<i>Removal of Property</i>	8
<i>Information Back-up</i>	8
<i>Fault logging</i>	8
RATIONALE	9
RISK	9
IMPACT	9
<i>Users</i>	9
<i>Data Owners</i>	9
<i>Managers</i>	9
<i>Application Development and Database Administrators</i>	10
<i>Help Desk</i>	10

Introduction

References

Regulatory

Insert Regulatory requirements

Security Standards

1. ISO 15408-2, Common Criteria, paragraph 11, Class FRU: Resource Utilization.
2. International Standard, Information Technology – Code of practice for Information Security Management, ISO/IEC 17799:2000(E), paragraph 7, Physical and Environmental Security and paragraph 8, Communications and Operations Management.
3. DoD Directive 5200.28, Trusted Computer System Evaluation Criteria, C2 Class Assurance Level.

Purpose

The purpose of establishing this Resource Utilization policy is to maximize the availability of the [ORGANIZATION] information data. Failures between the end-user and the desired data must be eliminated. This policy alleviates failures between end-users by implementing and maintaining a high level of fault tolerance, without making huge capital investments to the agency.

Scope

This policy illustrates that maintaining a high level of data access and maximizing a user's efficiency are two major concerns of the [ORGANIZATION]. This policy dictates that system administrators shall implement resource utilization solutions to greatly increase the overall availability of data by deploying robust fault tolerant systems from the data center to the desktop, featuring built-in redundancy and fault monitoring of the critical components used to store, manage and transfer data. This policy assures that sensitive information is properly safeguarded, and 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.

Resource Utilization Program

Fault Tolerance

To ensure resource utilization, system administrators shall invoke system redundancy capabilities on critical systems. This will mitigate the risk of degraded and limited fault tolerances enabling the correct operation of identified capabilities in the event of identified failures. System administrators will ensure that any failure detected is auditable.

Priority of Services

The system administrators shall implement effective mechanisms to control the use of resources within the [ORGANIZATION] by users and subjects such that the high priority activities within the [ORGANIZATION] will always be accomplished without undue interference or delay caused by low priority activities.

1. The system administrator shall assign a priority to each subject and that access shall be mediated on the basis of the subject's assigned priority; and
2. The system administrator shall assign a priority to each subject and that each access to all shareable resources shall be mediated on the basis of the subject's assigned priority.

Resource Allocation

To ensure resource allocation, where applicable, system administrators will identify and implement the principles and processes used to determine how computer resources for technology are allocated to meet the needs of the [ORGANIZATION]. These principles and processes shall control the use of resources by users and subjects such that denial of services shall not occur of unauthorized monopolization of resources. These services provided include access to the Internet, network disk space, information exchange or sharing of files, e-mail, printing, and backup of files. The system administrator shall set minimum and maximum quotas that will ensure users and subjects of having at least a minimum of a specified resource and that they will not monopolize a controlled resource.

Resource Utilization

To ensure resource utilization, equipment shall be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This shall also consider equipment siting and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure. All rejections of allocation operations due to resource limits shall be auditable.

Equipment Siting and Protection

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. This maximizes the availability of the [ORGANIZATION]'s informational data to the user. The following controls shall be considered:

1. Equipment shall be sited to minimize unnecessary access into work areas;
2. Information processing and storage facilities handling sensitive data shall be positioned to reduce the risk of overlooking during their use;
3. Items requiring special protection shall be isolated to reduce the general level of protection required;
4. Controls shall be adopted to minimize the risk of potential threats including:
 - a. Theft;
 - b. Fire;
 - c. Explosives;

- d. Smoke;
 - e. Water (or supply failure);
 - f. Dust;
 - g. Vibration;
 - h. Chemical effects;
 - i. Electrical supply interference; and
 - j. Electromagnetic radiation.
5. The [ORGANIZATION] shall put into place considerations towards eating and drinking in proximity to information processing facilities;
 6. Environmental conditions shall be monitored for conditions, which could adversely affect the operation of information processing facilities; and
 7. The impact of a disaster happening in nearby premises (e.g., water leaking from the roof or in floors below ground level or an explosion in the street) shall be considered.

Power Supplies

To ensure resource utilization availability is maximized to users, all equipment shall be protected from power failures and other electrical anomalies. A suitable electrical supply shall be provided that conforms to the equipment manufacturer's specifications.

1. Options to achieve continuity of power supplies include:
 - a. Multiple feeds to avoid a single point of failure in the power supply;
 - b. Uninterruptible power supply; and
 - c. Back-up generator.
2. An uninterruptible power supply to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Contingency plans shall cover the action to be taken on failure of the uninterruptible power supply. This equipment shall be regularly checked to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.
3. A Back-up generator shall be considered if processing is to continue in case of a prolonged power failure. If installed, generators shall be regularly tested in accordance with the manufacturer's instructions. An adequate supply of fuel shall be available to ensure that the generator can perform for a prolonged period.
4. In addition, emergency power switches shall be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting shall be provided in case of main power failure. Lighting protection shall be applied to all buildings and lighting protection filters shall be fitted to all external communications lines.

Cabling Security

To ensure resource utilization pertaining to communications, power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. The following controls shall be considered:

1. Power and telecommunications lines into information processing facilities shall be underground, where possible, or subject to adequate alternative protection;
2. Network cabling should be protected from unauthorized interception or damage, for example, by using conduit or by avoiding routes through public areas;
3. Power cables shall be segregated from communications cables to prevent interference; and
4. For sensitive or critical systems further controls to consider include:
 - a. Installation of armored conduit and locked rooms or boxes at inspection and termination points;
 - b. Use of alternative routings or transmission media;
 - c. Use of fiber optic cabling; and
 - d. Initiation of sweeps for unauthorized devices being attached to the cables.

Equipment Maintenance

Equipment shall be correctly maintained to ensure its continued availability and integrity. The following controls shall be considered:

1. Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications;
2. Only authorized maintenance or system administrator personnel shall carry out repairs and service equipment;
3. Records shall be kept of all suspected or actual faults and all preventive and corrective maintenance; and
4. Appropriate controls shall be taken when sending equipment off premises for maintenance (i.e., regarding deleted, erased and overwritten data). All requirements imposed by insurance policies shall be complied with.

Security of Equipment Off-Premises

Regardless of ownership, management shall authorize the use of any equipment outside the [ORGANIZATION]'s premises for information processing. The security provided should be equivalent to that for on-site equipment used for the same purpose, taking into account the risks of working outside the [ORGANIZATION]'s premises. Information processing equipment includes all forms of personal computers, organizers, mobile phones, paper or other form, which is held for home working or being transported away from the normal work location. The following guidelines shall be considered:

1. Equipment and media taken off the premises shall not be left unattended in public places. Portable computers shall be carried as hand luggage and disguised where possible when traveling.
2. Manufacturers' instructions for protecting equipment shall be observed at all times (e.g., protection against exposure to strong electromagnetic fields).
3. Home-working controls shall be determined by a risk assessment and suitable controls applied as appropriate (e.g. lockable filing cabinets, clear desk policy, and access controls for computers).
4. Adequate insurance coverage shall be in place to protect equipment off-site.

5. Security risks (e.g., of damage, theft and eavesdropping) may vary considerably between locations and shall be taken into account in determining the most appropriate controls.

Secure Disposal or Re-use of Equipment

Information can be compromised through careless disposal or re-use of equipment. Storage devices containing sensitive information shall be physically destroyed or securely overwritten rather than using the standard delete function. All items of equipment containing storage media, e.g. fixed hard disks, shall be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal. Damaged storage devices containing sensitive data may require a risk assessment to determine if the items shall be destroyed, repaired or discarded.

Removal of Property

Equipment, information or software shall not be taken off-site without authorization. Where necessary and appropriate, equipment shall be logged out and logged back in when returned. Spot checks shall be undertaken to detect unauthorized removal of property. Individuals shall be made aware that spot checks will take place.

Information Back-up

Back-up copies of essential business information and software shall be taken regularly. Adequate back-up facilities shall be provided to ensure that all essential business information and software could be recovered following a disaster or media failure. Back-up arrangements for individual systems shall be regularly tested to ensure that they meet the requirements of business continuity plans. The following controls shall be considered:

1. A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. At least three generations or cycles of back-up information shall be retained for important business applications.
2. Back-up information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site shall be extended to cover the back-up site.
3. Back-up media shall be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.
4. Restoration procedures shall be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
5. The retention period for essential business information, and also any requirement for archive copies to be permanently retained, shall be determined.

Fault logging

Faults shall be reported and corrective action taken to ensure continuance of resource allocation and utilization within the [ORGANIZATION]. Faults reported by users regarding problems with information processing or communications systems shall be logged. There shall be clear rules for handling reported faults including:

1. Review of fault logs to ensure that faults have been satisfactorily resolved; and
2. Review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

Rationale

This policy provides authority for the implementation of information management resource utilization and allocation strategies, procedures, and practices needed to control and manage the [ORGANIZATION]'s resources in order to meet business, legal and fiscal requirements and to measure the effectiveness of information management systems and programs.

As the [ORGANIZATION] develops and expands its networks and enterprise infrastructures to incorporate the Internet, intranets, and e-commerce, resource utilization and allocation increases dramatically -- as does the need for integrated and centralized resource management. The Information Systems Division is expected to maintain applications and services outside the traditional data center with the same level of predictability that users have come to expect from services that were originally inside the data center.

Risk

Failure to comply with this stated policy may place the [ORGANIZATION] in irreparable harm. The [ORGANIZATION]'s business continuity is, of course, a vital activity. Failure to implement resource utilization and allocation solutions into the [ORGANIZATION] network alleviates the protection against security threats, such as interception, interruption, modification, and fabrication.

Impact

All areas of the [ORGANIZATION] shall comply with this resource utilization 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 who have access to the [ORGANIZATION]'s network or systems. This policy illustrates that the [ORGANIZATION] holds the individual user accountable and responsible for ensuring that information data and resources are readily available.

Data Owners

This policy assists the data owners in assuring that only authorized users have access and that unauthorized access will be determined and prevented when possible.

Managers

This policy shall allow management to take appropriate action to ensure that resource utilization and allocation solutions are implemented to ensure that information data and resources are readily available within the [ORGANIZATION]. This policy allows management to initiate or

direct the development of a procedure for emergency access to information in the event of a crisis, and the unavailability of critical resources or assets to gain access to the information.

Application Development and Database Administrators

System administrators are responsible for implementing and monitor resource utilization and allocation solutions to ensure that the availability of critical resources or assets is readily available to all users within the [ORGANIZATION].

Help Desk

The Help Desk needs to ensure that continuity of access control to critical resources or assets are readily available to all users within the [ORGANIZATION].