

# SECURITY POLICY

## SECURITY AUDIT

### **This is a copyrighted document**

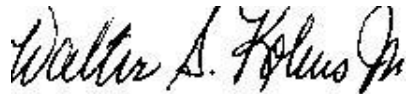
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your ORGANIZATION then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright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

<b>INTRODUCTION .....</b>	<b>4</b>
REFERENCES.....	4
<i>Regulatory</i> .....	4
<i>Security Standards</i> .....	4
PURPOSE.....	4
SCOPE.....	4
<b>AUDITING.....</b>	<b>5</b>
POLICY .....	5
<i>Audit Trails</i> .....	5
<i>Logging</i> .....	5
<i>Security of the Audit</i> .....	6
<i>Audit and Variance Detection Controls</i> .....	6
<i>Security Alarms</i> .....	7
RATIONALE .....	8
RISK .....	8
IMPACT .....	8
<i>Users</i> .....	8
<i>Data Owners</i> .....	8
<i>Managers</i> .....	8
<i>Infrastructure</i> .....	8
<i>Network</i> .....	8
<i>Application Development/Database Administrator's</i> .....	9
<i>Hardware</i> .....	9

## **Introduction**

### ***References***

#### *Regulatory*

1. Insert regulatory requirements.

#### *Security Standards*

1. Sarbanes-Oxley Act
2. Requirements, ISO/ECI, 15408, Common Criteria, paragraph 3, Class FAU: Security Audit.
3. International Standard, Information Technology – Code of practice for Information Security Management, ISO/ECI 17799:2000(E), paragraph 9.7 and 12.3.
4. DoD Directive 5200.28, Trusted Computer System Evaluation Criteria, C2 Class Assurance Level.

### ***Purpose***

The purpose of establishing this Audit policy is to detect and deter penetration of any [ORGANIZATION] computer system and to reveal usage that identifies misuse. Audits may be conducted to:

- Ensure integrity (the modification or destruction of data on servers and during transmission), confidentiality, and availability (preventing denial of service attack, etc.) by reviewing and maintaining audit logs;
- Investigate possible security incidents and ensuring conformance to [ORGANIZATION] security policies;
- Monitor user or system activity where appropriate to prevent unauthorized browsing or disclosure of any tax return or tax return information;
- Ensure that systems logs are established and maintained on access to sensitive information such as tax return, tax return information, critical systems, and appropriate devices;
- Ensure that access to audit logs is restricted and a separation of duties is maintained;
- Ensure the handling of sensitive information is restricted to authorized personnel;
- Ensure that Audit logs are reviewed on a recurring basis with the ability to do selective auditing of information by exception; and
- Ensure audit logs are archived for future references.

### ***Scope***

This policy covers all individuals responsible and accountable for the protection of sensitive information computer and communication devices owned or operated by [ORGANIZATION]. This policy also covers any computer and communication devices that are present on [ORGANIZATION] premises, but which may not be owned or operated by the [ORGANIZATION]. Assures taxpayers that 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. The

security standards require that a user's actions be open to scrutiny by means of an audit. The audit process of a secure system is the process of recording, examining, and reviewing any or all security-relevant activities on the system to assess the risks of loss, compromise, or damage to sensitive information. This policy establishes issues involved in implementing and evaluating an audit mechanism.

- The scope of internal auditing work, as specified in this policy, encompasses what audit work should be performed. It is recognized, however, that Executive management and the Commissioner provide general direction as to the scope of work and the activities to be audited;
- The purpose of the review for adequacy of the system of internal control is to ascertain whether the system established provides reasonable assurance that the [ORGANIZATION]'s objectives and goals will be met efficiently and economically;
- The purpose of the review for effectiveness of the system of internal control is to ascertain whether the system is functioning as intended;
- The purpose of the review for quality of performance is to ascertain whether the [ORGANIZATION]'s objectives and goals have been achieved; and
- The primary objectives of internal controls are to ensure:
  1. Reliability and integrity of information;
  2. Compliance with policies, plans, procedures, laws, and regulations;
  3. Safeguarding of assets;
  4. Economical and efficient use of resources; and
  5. Accomplishment of established objectives and goals for operations or programs.

## **Auditing**

### ***Policy***

#### *Audit Trails*

The [ORGANIZATION] must maintain audit trail records in compliance with various regulatory laws, rules, and guidelines. This policy sets internal controls and audit requirements to include: individual accountability, reconstructing event, problem monitoring, and intrusion detection tools to monitor sensitive systems.

#### *Logging*

All access to networked systems must be logged. When determined to be critical to the [ORGANIZATION], the logging of transactions must be included regardless of the operating platform. Log data must be classified as sensitive. These logs must be retrievable through clearly defined procedures and must be maintained for time periods prescribed for audit, legal, and recovery purposes. As new applications, platforms, mediums, or other technical changes to system operations are made; consideration of logging requirements and availability must be made. Requirements for logging data must be clearly established as system, architectural, technical, or network designs.

### *Security of the Audit*

Audit trail software, as well as the audit trail, and settings itself, should be protected by a trusted computing baseline and should be subject to strict management, operational, and technical access controls. The security requirements of the audit mechanism are the following:

1. The event recording mechanism shall be part of a trusted computer baseline and shall be strictly controlled from unauthorized modification or circumvention;
2. Audit trail information shall be protected as sensitive information by a trusted computer baseline from unauthorized access (i.e., users read access to the audit records shall be prohibited, except those users or authorized personnel that have been granted explicit read-access). Separation of duties will be enforced where the authorized user reviewing the audit trails will not have the ability to modify the audit results; and
3. The audit-event enabling/disabling mechanism shall be part of a trusted computer baseline and shall remain inaccessible to unauthorized users.

At a minimum, the data on the audit trail should be considered to be sensitive, and the audit trail itself shall be considered to be as sensitive as the most sensitive data contained in the system. When the medium containing the audit trail is physically removed from the trusted computer platform, the medium should be accorded the physical protection required for the highest sensitivity level of data contained in the system.

### *Audit and Variance Detection Controls*

Audit and variance detection controls must allow executive management or representatives to conduct an independent review of records and activities to test the representative adequacy of system, application controls, and to detect/react to departures from established policies, rules, and procedures. Variance detection includes the use of system logs and audit trails. For an application, variance detection checks for anomalies in user or system behavior, in such things as the numbers and types of transactions, volume and dollar thresholds, access outside normal work hours and other deviations from standard activity profile. These reviews may provide early detection of unauthorized system or application access attempts as well as contaminated software (erroneous or malicious programs or computer viruses).

Two basic types of reviews fit into this category of controls—system audits and security monitoring:

1. System audits are “snapshot” analyses of applications at a specific point in time. Self-administered system reviews shall be established on a recurring basis during the year and performed by internal staff. Self-reviews shall be documented to allow independent auditors to evaluate the methodology, timeliness, and results; and
2. Security monitoring is an ongoing activity that is intended to identify vulnerabilities, deviations from established security procedures, and other security concerns. Monitoring is similar to system review in that many of the same analytical procedures are used. System monitoring, however, is performed more regularly and is more likely to identify minor or transitory events that may be indicative of potential security intrusions, threats, or weaknesses. System monitoring tools are typically used to assist security-monitoring

tools for “real time” analysis. The type of system monitoring, results, frequency, and tools used shall be documented for review by independent audits.

All systems that process sensitive information or are considered critical to the [ORGANIZATION] operation must provide for the following audit control functionality.

The audit control function shall be able to generate an audit record of the following auditable events:

1. Start-up and shutdown of the audit functions;
2. All auditable events for the level of audit required by the Auditor;
3. The audit control function as a minimum shall record within each audit record the date and time of the event, type of event, subject identity, objective identity, and the outcome (success or failure) of the event. Special consideration should be given when designing audit control function on federal tax information to include, user’s identity, SSN of the taxpayer account accessed, type of taxpayer (individual or business), event code (what was done) researched / adjusted account / etc., tax period involved, and date and time of access;
4. The audit control function will allow the comparison of the signature events and event sequences against the record of system activity;
5. The audit control function shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation;
6. The audit control function shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access;
7. The audit control function shall provide the audit records in a manner suitable for the user to interpret the information;
8. The audit control function shall provide the ability to perform searches of audit database on criteria with logical relationships;
9. The audit control function shall be able to include or exclude auditable events from the set of audited events based on object identity, user identity, subject identity, and host identity;
10. The audit control function shall protect the stored audit records from unauthorized deletion;
11. The audit control function shall be able to prevent modifications to the audit records;
12. The audit control function shall ensure that audit records will be maintained when audit storage is exhausted, fails, or an attack has occurred; and
13. Those authorized users, which have a role as administrator of a network device, operating system, or security software such as a firewall, Intrusion Detection System, etc., will have all events logged.

#### *Security Alarms*

Managers will ensure that an individual shall be given the responsibility to develop a list of the least disruptive actions upon detection of a potential security violation. These actions will be documented and used to assist in reporting security incidents.

## ***Rationale***

Auditing is a control, which functions by examining and evaluating the adequacy and effectiveness of other controls throughout the [ORGANIZATION]'s critical infrastructure to prevent loss, modification, or misuse of user data in application systems. Appropriate controls and audit trails or activity logs should be designed into application systems, including user written applications. These should include the validation of input data, internal processing and output data. Records should be categorized into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys associated with encrypted archives or digital signatures, should be kept securely and made available to authorized persons when needed.

## ***Risk***

If audit trail capability is not provided, then the ability to analyze and trace security problems will be severely limited and not meet the legal requirements of both Federal and State laws. Failure to meet this security requirement could cause loss of [ORGANIZATION] information sharing with the Internal Revenue Service. Unauthorized browsing of sensitive information could cause employees, managers, and executives to be individually fined and dismissed.

## ***Impact***

### *Users*

This policy shall impact all users that have access to sensitive data and provides the knowledge that such access is recorded and holds the individual user accountable and responsible for unauthorized access.

### *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 will provide the ability to take appropriate action on those employees that perform unauthorized access to sensitive information.

### *Infrastructure*

Working with Application Managers and Data Owners ensure that proper audit trails are maintained, reviewed, and archived on all servers that process or store sensitive information.

### *Network*

Ensure that audit logs are maintained, reviewed, and archived on all network devices, firewalls, etc.

*Application Development/Database Administrator's*

Ensure that all sensitive applications have the appropriate audit functions to abide by Federal laws, State laws, and policies.

*Hardware*

This policy could impact on hardware resources such as network devices (i.e. Increased traffic), more powerful servers, additional disk space, and higher processor utilization.