

# SECURITY POLICY

## CERTIFICATION AND ACCREDITATION OF SENSITIVE INFORMATION PROCESSING APPLICATIONS AND GENERAL SUPPORT SYSTEMS

### THIS IS A COPYRIGHTED DOCUMENT.

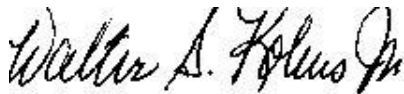
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your organization then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright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

1. Fill out the Clearance Document and sign it; and
2. 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:

1. 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.
2. Performance and Display Rights. RECIPIENT may not display any TESS Templates in public in any media format.
3. Exclusive or Nonexclusive. RECIPIENT has nonexclusive permission of the following Template(s) \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_.
4. 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:
  - a. Mutual agreement of the parties to terminate the Agreement.
  - b. 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.
5. 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.
6. 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>5</b>
REFERENCES .....	5
<i>Regulatory</i> .....	5
<i>Security Standards</i> .....	5
POLICY .....	5
SCOPE .....	5
<i>Accreditation</i> .....	5
<i>Certification</i> .....	6
<i>Vulnerability Assessment and Testing</i> .....	6
<i>Acceptance</i> .....	6
POLICY .....	7
<i>Assistant Commissioner for Technology</i> .....	8
<i>Data Owner</i> .....	8
<i>Certification Committee Team Members</i> .....	8
<i>Information Security Professional</i> .....	8
<i>Certification Chairperson</i> .....	9
<i>Information Security Officer</i> .....	9
<i>Application Project Manager</i> .....	9
<i>Data Owner or Representative</i> .....	9
<i>The Data Owner or Representative shall have the following roles:</i> .....	9
<i>Quality Assurance Analyst</i> .....	9
RE-CERTIFICATION AND RE-ACCREDITATION .....	10
<i>Changes to the System</i> .....	10
<i>Changes in Requirements</i> .....	10
<i>Passage of a Time Interval</i> .....	10
<i>Occurrence of a Significant Violation</i> .....	10
<i>Audits or Review Findings</i> .....	11

**EXHIBIT 1 - SECURITY CERTIFICATION PACKAGE FORMAT .....12**  
**EXHIBIT 2 - SAMPLE CERTIFICATION LETTER RECOMMENDING IMPLEMENTATION .....13**  
**EXHIBIT 3 - SAMPLE CERTIFICATION LETTER WITH SIGNIFICANT RISKS .....14**  
**EXHIBIT 4 - SAMPLE ACCREDITATION LETTER TO DATA OWNER .....15**  
**EXHIBIT 5 - SAMPLE ACCREDITATION LETTER WITH SIGNIFICANT RISKS ..... 16**

## Introduction

### References

#### *Regulatory*

1. *List applicable regulatory laws*

#### *Security Standards*

1. ISO 15408-3, Common Criteria, paragraph 8, Class ACM: Configuration Management.
2. ISO 15408-3, Common Criteria, paragraph 9, Class ADO: Delivery and Operation.
3. ISO 15408-3, Common Criteria, paragraph 10, Class ADV: Development.
4. ISO 15408-3, Common Criteria, paragraph 12, Class ALC: Life Cycle Support.
5. ISO 15408-3, Common Criteria, paragraph 13, Class ATE: Tests.
6. ISO 15408-3, Common Criteria, paragraph 14, Class AVA: Vulnerability Assessment.
7. International Standard, Information Technology – Code of practice for Information Security Management, ISO/IEC 17799:2000(E), paragraph 10.1, Security Requirements of Systems.
8. Sarbanes-Oxley Act
9. Cobit
10. COSO
11. HIPAA
12. G-B-L

### Policy

This policy defines requirements for assurance through the adoption of a well-defined life-cycle model for all steps of development, including flaw remediation procedures and policies, correct use of tools, techniques, processes, and the security baseline measures used to protect the development environment. It further outlines responsibilities to ensure that sensitive Information Processing Application and General Support Systems meet security requirements and comply with federal and state laws and directives on information systems security.

The Certification and Accreditation life cycle process serves to ensure that the security functions of a developed system meet the needs of protecting that system and its information, and that implementation decisions are made with full consideration of security factors. The term *system* shall be used throughout this policy to refer to any General Support System or sensitive Information Processing Application being developed for operation within the [ORGANIZATION]. This concept applies whether the system is a complete computer and communication system with its own hardware or is a new application to be run on an existing platform.

### Scope

#### *Accreditation*

Accreditation is the official management authorization to operate a system. An accreditation normally grants approval for a system to operate for a specific period of time, in a defined environment, and with defined security measures and other appropriate restrictions. The accreditor formally accepts security responsibility for the system and declares that the protection

mechanisms against compromise, destruction, or unauthorized modification are adequate. Since no information system is ever totally secure, accreditation documents the accreditor's judgment that the benefits of operating the system are worth the residual risks that are involved. The [ORGANIZATION] Senior Manager (Data Owner) will make this accreditation decision.

### *Certification*

Certification is the comprehensive analysis of the security aspects of the system to establish the extent to which the system meets its security requirements (see Figure 1). It is an application risk assessment that produces a technical opinion and supporting information. The accreditor in making the decision uses the resulting documentation. To make such a judgment, the accreditor needs reliable information about the system. This information includes likely threats or ways the system might be misused, the specific portions of the system or data, which need protection, the mechanisms used to provide protection, and how well those mechanisms operate. This is the point of the certification.

### *Vulnerability Assessment and Testing*

The agency will perform both Unit Tests and Acceptance Tests, and will certify that the security controls are adequate for security needs.

1. The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the network as described in the functional specification.
2. The test coverage shall rigorously demonstrate that all external interfaces of the [ORGANIZATION] network identified in the functional specification have been completely tested.
3. The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the network operates in accordance with its sensitive high-level and low-level design.
4. The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
5. The developer shall test and document that a systematic method was used to identify covert channels for each information flow control policy.
6. The testing shall identify discretionary modes of operation of the network (including operation following failure or operational error), their consequences and implications for maintaining sensitive operation.
7. A quantitative or statistical analysis of the security behavior shall to identify any vulnerability that could bypass, deactivate, or corrupt a security function or a security mechanism
8. A penetration test, based on the vulnerability analysis, shall determine the exploitability of additional identified vulnerabilities in the intended environment.

### *Acceptance*

The final step in the [ORGANIZATION] process is acceptance of the system by the Data Owner. The Data Owner will review the entire system after development and testing, including the Certification and Accreditation information, and will either accept or reject the system as delivered (see Figure 1).

For information systems developed for and by the [ORGANIZATION], certification activities begin at the inception of the system development and proceed throughout the life cycle of the system. A certification team, whose core members shall be assigned during the system-planning phase, shall perform certification. Additional members may be added later during system development. This team must be an integral part of the system development team and shall participate fully in all phases of development. In this way, the team can ensure that security issues are recognized, addressed, and resolved at the earliest possible point in development, when changes can be made at the lowest cost. Specifically, the certification team shall:

1. Collect existing documents;
2. Review development documents in each phase for security aspects;
3. Build the certification package that will:
  - a. Describe in brief the system and its sensitivity;
  - b. Summarize protection requirements, vulnerabilities, and security features needed; and
  - c. Summarize security relevant tests, test results, and residual risks.
4. Forward the certification package, with cover letter highlighting the findings, to the Assistant Commissioner for Technology.

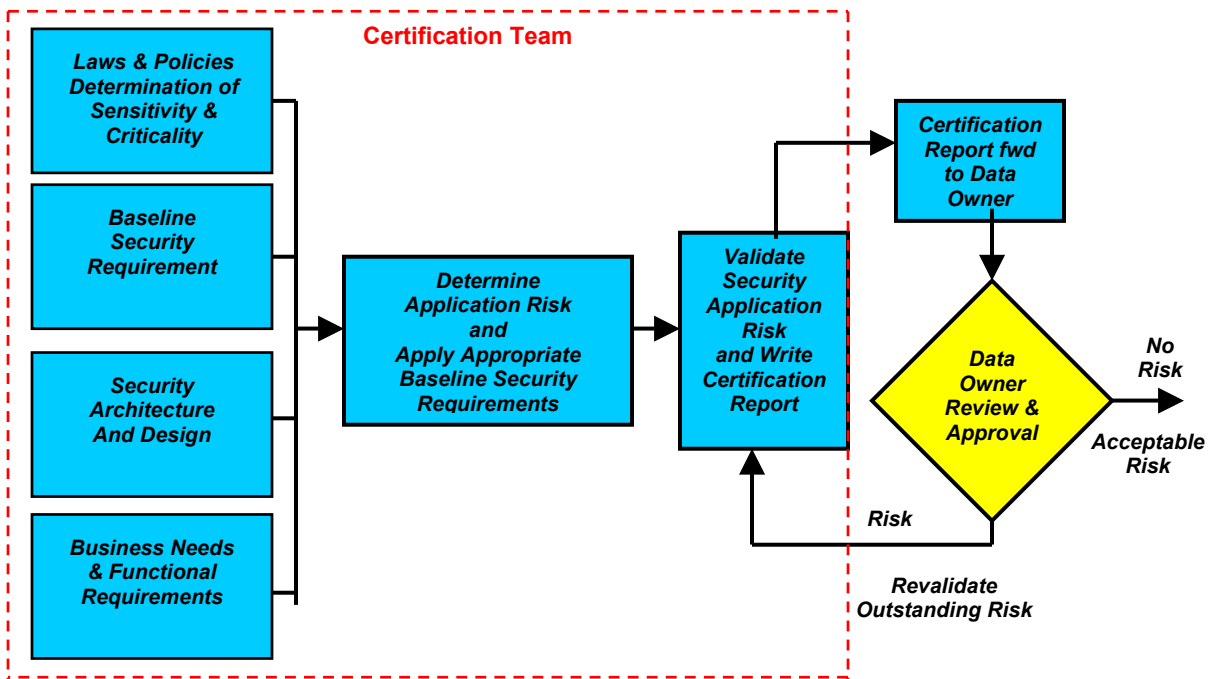


Figure 1 – Certification and Accreditation in the Development Life Cycle

## Policy

This section identifies and describes the key roles involved in managing the security certification and accreditation process. The certification and accreditation authorities are identified and their major responsibilities listed.

#### *Assistant Commissioner for Technology*

The Assistant Commissioner for Technology will perform the role of Certifier. Both the certification committee chairperson, a member from the security team and the Information Security Officer prior to transmittal to the Assistant Commissioner for Technology will sign the certification package (see Exhibit 1).

#### *Data Owner*

The Data Owner will perform the role of Certifier. The ultimate decision to accept and use the system belongs to the Data Owner for the information that will be stored or processed on that information processing application. When more than one Data Owner's information is involved each affected Data Owner will be required to sign off on acceptance. This acceptance decision is based on many considerations, including the security factors that are described in the Certification Package. Specific roles of the Data Owner are as follows:

1. Determine system sensitivity and criticality;
2. Be a member or assign a representative to certification team;
3. Review the Certification Package from the Assistant Commissioner of Technology as part of system acceptance; and
4. Accept or reject the system for implementation and production.

#### *Certification Committee Team Members*

The core membership of the certification committee shall be assigned normally at the beginning of the planning phase and must be an integral part of the development life cycle process. The core members of the certification committee are:

1. Information Security Professional
2. Quality Assurance Analyst
3. Application Project Manager
4. Data Owner or representative

#### *Information Security Professional*

The Information Security Professional shall be the leader of the certification team and designated as the Chairperson. Other subject matter experts (e.g., legal expert, operations representative, and system designer) can be added to the team at appropriate times in the process, if warranted. Specific roles of the certification membership are:

1. Review and approve the security related project documents at each phase during development life cycle;
2. Build the certification package using appropriate project documents;
3. Identify needs for additional subject matter experts on the team;
4. Forward certification package documents in sufficient time to assemble certification package with cover letter to the Information Security Officer; and

5. Implement configuration management automated tools ensuring all changes are authorized and logged, version numbers are tracked, and auditing capabilities are turned on.

#### *Certification Chairperson*

The certification chairperson shall perform the role of documenting the certification package and findings. The Chairperson shall then forward the certification package to the Information Security Officer for review and approval of findings. The certification team shall throughout the development life cycle:

1. Identify security issues early;
2. Correct and resolve problems early where costs are lower; and
3. Ensure, if possible, that all risks are mitigated prior to implementation and production. For risks that are not mitigated provide compensating controls and recommendations to resolve outstanding risk that cannot be resolved.

#### *Information Security Officer*

The Information Security Officer, as the manager of the Enterprise Information Security Group, shall have the following roles:

1. Assist Data Owner as requested in reviewing sensitivity determinations both as the Privacy and Information Security Officer for the [ORGANIZATION]; and
2. Assign an Information Security Professional as the Chairperson to the Certification Committee.

#### *Application Project Manager*

The Application Project Manager shall have the following roles:

1. Be a member of the Certification Committee;
2. Ensure that security requirements for which the Application Project Manager is responsible are completed;
3. Ensure that security requirements that require coordination with other groups are accomplished; and
4. Assign additional subject matter experts to the certification committee as required.

#### *Data Owner or Representative*

The Data Owner or Representative shall have the following roles:

1. Be a member of the Certification Committee; and
2. Ensure that the security requirements are met to the Data Owner information classification and criticality.

#### *Quality Assurance Analyst*

The Quality Assurance Analyst shall have the following roles:

1. Be a member of the Certification Committee; and

2. Ensure that the security requirements are tested and validated to meet the Data Owners information classification and criticality.

***Re-certification and Re-accreditation***

Certification and accreditation are not permanent. As a system or its security environment changes, re-certification and re-accreditation are needed to verify that security protection remains acceptable to the [ORGANIZATION] security policy. Any change or new finding that invalidates or calls into question an accreditation decision necessitates re-certification and re-accreditation. Situations that give rise to this include the following:

*Changes to the System*

For sensitive systems, all changes large and small should be closely controlled. These various changes give rise to “levels” of re-certification and re-accreditation in which, for example, small changes are controlled by a change control process while large changes may require a full re-certification and re-accreditation process (see Table 1).

<b>Level</b>	<b>Nature of Change</b>	<b>Accrediting Official(s)</b>	<b>Certification Process</b>
1	Major; affecting the basic security design.	Original Accreditation Official(s)	Full certification process; re-certify entire system including portions that have not changed.
2	Intermediate; moderate change affecting two or more security requirements; addition or change of major hardware component.	Data Owner	Partial process involving only the areas of change; formal acceptance test plan and independent testing required for relevant security requirements
3	Minor, within one security requirement and affecting no other	Change Control Board	Normal change control processing; no formal acceptance test plan or independent testing required

Table 1 - Re-certification Levels

*Changes in Requirements*

This includes changes in state, federal, and the [ORGANIZATION] security practices and in user requirements. (e.g., the need to process data of a higher sensitivity). Requirement changes also include altering definitions of “good practice” as reflected in the literature or as interpreted by the courts. All of these changes raise the question of whether system safeguards satisfy the altered requirements. This question is formally addressed by re-certification and re-accreditation.

*Passage of a Time Interval*

Three years shall be the maximum interval between re-certification and re-accreditation. Highly sensitive systems might require annual re-certification and re-accreditation. Time intervals can also trigger follow-up evaluations for corrections.

*Occurrence of a Significant Violation*

A violation or incident that calls into question the findings of a prior certification may require that the system be re-certified and reaccredited. If the system has never been accredited, a major violation might supply the needed impetus to do so.

*Audits or Review Findings*

A re-certification might be triggered based on findings deriving from an audit, an external security review, spot-check, risk analysis, vulnerability assessment or internal control review, or some other source.

## Exhibit 1 - Security Certification Package Format

The security certification package provides to the accreditors the information they need to understand the security issues and risks involved and to make the accreditation decision. It contains the following parts and information:

- *System Certification Letter.* This letter, addressed to the accreditors, serves as the cover letter and executive summary for the certification package. It contains the committee's recommendation for accreditation including necessary environmental and administrative restrictions. The certification chairperson must sign the letter. When appropriate, committee members may attach dissenting opinions for the consideration of the accreditors.
- *Introduction.* This section briefly describes the project and its environment for development and Certification and Accreditation. It identifies the sponsor and the developing organization and makes reference to key project development documents. It summarizes the development timeline and intended operating environment for the project. It also lists the name, title, and organization of the accreditors and the members of the Certification Committee.
- *Security Synopsis.* This section provides a brief overview of the security relevant aspects of the system. It includes a summary of the security requirements that identifies the components of the system that require protection and the type of protection needed. Detailed security requirement sheets are provided for reference as an appendix. It also describes the primary methods, including physical, administrative, and technical controls that provide the desired protection.
- *Evaluation Approach.* This section describes the approach to be used in evaluating the degree to which the system meets its security requirements. It defines the areas to be focused on during testing, the evaluation criteria, and the specific test methods to be used. Specific tasking and support requirements for accomplishing the evaluation may also be included.
- *Test Results Summary.* This section provides a summary description of the types of security tests performed on the system and the results of the tests. It should contain sufficient detail to highlight for the accreditors how well each of the system components described in the synopsis are protected and to what degree the system security requirements have been met. Detailed test procedures and actual results are included for reference as an appendix.
- *Residual Risks.* This description, based on the testing results and the committee's knowledge of the system, identifies security risks that remain after consideration of the security mechanisms in place. It should enumerate the nature of the threats or attacks to which the system is still vulnerable and the likely consequences should such an attack be successful. Recommendations for corrective actions or procedures to reduce the residual risks may also be included.

## **Exhibit 2 - Sample Certification Letter Recommending Implementation**

[Date]

Chief Information Officer

SUBJECT: Security Certification for [Project Name]

Attached is the Security Certification Package for [Project Name]. The specific security requirements, operating environment, security measures, and test results are detailed in the package and summarized below.

The primary security concerns within [Project Name] are protection from system disruption and disclosure of taxpayer data. The system will be executed on a local area network that is totally contained within a physically secure area. The only connection to other networks is through a carefully configured firewall, and intrusion detection software is installed as an added precaution. Attempts to access sensitive data through the firewall found no apparent vulnerabilities.

The certification committee finds no risk and recommends that [Project Name] be accredited for operation within the described environment for the next 3 years, subject to continued use of the administrative and configuration controls that are now part of the system and are described in the attached package.

[Signature]

Committee Chairperson

[Signature]

Information Security Officer

Attachment

Security Certification Package

### **Exhibit 3 - Sample Certification Letter with Significant Risks**

[Date]

Chief Information Officer

SUBJECT: Security Certification for [Project Name]

Attached is the Security Certification Package for [Project Name]. The specific security requirements, operating environment, security measures, and test results are detailed in the package and summarized below.

The primary security concerns within [Project Name] are protection from system disruption and disclosure of taxpayer data. The system will be executed on a local area network within a public access building. There is a connection to the [ORGANIZATION] network through a firewall.

The certification committee has identified several vulnerabilities that present significant security risks. First, network access controls are not sufficient to prevent access by unauthorized personnel in the public building. Second, the firewall can be easily circumvented, as revealed by a penetration test.

We therefore recommend that [Project Name] not be accredited for operation at this time, pending corrective action. Possible actions might include reconfiguration of the firewall and more rigorous use of network access control mechanisms. Alternately, the system could be relocated to a more secure network.

[Signature]

Committee Chairperson

[Signature]

Information Security Officer

Attachment

Security Certification Package

## **Exhibit 4 - Sample Accreditation Letter to Data Owner**

[Date]

[Data Owner]

SUBJECT: Security Accreditation for [Project Name]

Information Systems management has reviewed the security aspects of [Project Name] as described in the attached Security Certification Package and has determined that the system's anticipated operation does not present unacceptable risks to the [ORGANIZATION] assets. Accordingly, [Project Name] is accredited for operation within the [ORGANIZATION] subject to your acceptance of the system as delivered.

This accreditation is for a 3-year period, at the end of which time the system will be examined to ensure that the security of the system has not been altered (for example, by change in the operating environment or by an increased threat).

This accreditation is also contingent on continued use of the administrative and configuration controls that are now part of the system and are described in the attached package.

[Signature]

Chief Information Officer

Attachment

Security Certification Package

cc: Certification Committee Chairman  
Information Security Officer

## **Exhibit 5 - Sample Accreditation Letter with Significant Risks**

[Date]

[/Data Owner]

SUBJECT: Security Accreditation for [Project Name]

Information Systems management has reviewed the security aspects of [Project Name] as described in the attached Security Certification Package. The operation of this system presents significant risks to the [ORGANIZATION] assets and we do not recommend implementation of the system at this time.

As currently designed and configured the system and its data are vulnerable to unauthorized access through network connections or physical access to system components. This could lead to costly system disruptions or improper release of sensitive data with probable legal consequences. Potential corrective actions would involve more rigorous configuration control and redesign of key system components.

Further information and assistance can be obtained from the Information Security Officer.

[Signature]

Chief Information Officer

Attachment

Security Certification Package

cc: Certification Committee Chairman  
Information Security Officer