
Applications Security Checklist

This is a copyrighted document

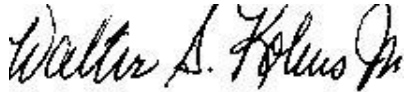
If you decide that you want to download this document and use it “as is” or make an adaptation (called Derivative Works) of the Template for use in your ORGANIZATION then you must pay a small fee of five dollars. This fee is charged for services for maintaining this document and processing copyright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

Recipient
By: _____

Walter S. Kobus Jr., VP

Print Name: _____

Date: _____

Date: _____

Item	Requirements/Controls	N/A	Yes	No
1	How is application development done in the organization? <input type="checkbox"/> In-house %, <input type="checkbox"/> Contracted out %, <input type="checkbox"/> Off shore %, <input type="checkbox"/> COTS %			
2	In development projects have all vendor licenses and copyrights been obtained that will be used in the development and production environment?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Is a Business Impact Analysis completed by the data-owner on applications prior to production and maintain up-to-date?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Is the agency database of applications updated to reflect sensitivity, criticality, and recover time?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	Does the development project manager take the appropriate reporting and corrective action when there has been a security incident?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	Have all security incidents that have occurred during the design, development, and testing been reported, documented, and resolved?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	Are independent or software validation code reviews being conducted on external Web application?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	Does the development team leader ensure that the data center is provided with appropriate backup and recovery procedures?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	Does the application development team follow a software development life cycle that contains validation and verification of security requirements and controls in each stage of development?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	Is the implementation of changes strictly controlled by the use of formal change control procedures?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	For each new application being developed, is the development platform security at the same level that it will be required in a production environment?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	Is security awareness training conducted for team members at beginning of each new development project?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	Have all security issues that have occurred during design, development, and testing been reported, documented, and resolved?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	Does the development team follow secure coding practices?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	Are copies of sensitive or critical applications documentation under development and secured when not in use by development staff members?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	Has the development team leader ensured that the targeted platform has the physical security controls required of the application being developed?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17	Has the development team leader ensured that the site risk assessment for both the development and production environment matches the security profile of the application being developed?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18	Is each application being developed coordinated with operations to ensure that the backup and recovery plan is updated to include the new applications requirements?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19	Are employees only capable of pulling up applications and systems needed to perform their current duty assignments?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20	Is there a design team for all application development, which includes a representative from network, operations, data owner, security, and development?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21	Is security part of the development life cycle project plan?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22	Does the development team leader ensure that all operations documentation is accomplished prior to production?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23	Are all versions to production program changes done using an approved change control process?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
24	Has the security architecture of all newly developed applications been approved by the Enterprise Security Architect?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
25	Are security milestones defined in each application development project?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
26	Is there a clear separation of duties to prevent project management controls from being overlooked?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27	On sensitive or critical application under development is a security risk assessment provided to the data owner for his approval prior to placing the application/COTS into production?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
28	Does each sensitive and critical application project have a security risk assessment committee assigned to it to ensure appropriate security requirements/controls are in place?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
29	Are peer code reviews being done on sensitive and critical applications being developed?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
30	If sensitive production data is used for test data has it either been scrubbed or moved into a test environment as secure as the targeted production environment and with a plan and the approval of the data owner, operation manager, and security?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
31	Are all outputs (screens, reports, etc) that contain sensitive information labeled e.g. "Confidential Information"?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

32	Is the development environment on sensitive or critical applications limited to only those that have a need to know?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
33	On critical applications, does the development team leader ensure that the contingency and disaster plan is updated?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Name (Print): _____ **Signature:** _____ **Date:** _____