Information Technology Application Security Plan

for Major Applications[1]

<Project or System Name> for <Name of Agency>

State of Alaska
State Security Office
Enterprise Technology Services

Month, Year

[1] *A Major Application is an information system that requires special management attention because of its importance and criticality to an agency mission; or because of its significant required investment in development, operation, or maintenance. A Major Application may significantly enable business and service delivery of agency programs, support fiscal processes, or manage property and other resources.*

Revision Sheet

Release No.	Date	Revision Description
Rev. 0	1/9/2015	Initial Draft
Rev. 1	1/9/2015	Various updates for readability and presentation

Major Application Security Plan Authorization Memorandum

I have carefully assessed the Major Application Security Plan for the *<Project or System Name>*.

MANAGEMENT CERTIFICATION - Please check the appropriate statement.

______ The document is accepted.

______ The document is accepted pending the changes noted.

______ The document is not accepted.

We fully accept the responsibility for mitigating security concerns raised by the State Security Office. The suggestions and advice provided will be thoughtfully considered as possible improvements in either system, application, or business process. We authorize initiation of work necessary to proceed in ensuring system security is in place at assessed level of baseline security control as informed by the Information System Categorization. Based on our authority and judgment, the operation of this system is authorized.

______________________________ ____________________
NAME DATE
Project/System Implementation Leader

______________________________ ____________________
NAME DATE
Program Area/Section/Sponsor or Representative

______________________________ ____________________
NAME DATE
Program Division/Sponsor or Representative

______________________________ ____________________
NAME DATE
Administrative Division Director or Representative

______________________________ ____________________
NAME DATE
Agency Information Security Officer (ISO)

GENERAL SUPPORT
SYSTEM SECURITY PLAN

TABLE OF CONTENTS

1.0 GENERAL INFORMATION

1.0 GENERAL INFORMATION

SYSTEM IDENTIFICATION

System Name/Title

- Unique Identifier & Name Given to the System.

Description of Information Sensitivity

- Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is: **High, Medium, or Low**.
- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system..

	Potential Impact		
Security Objective	**Low**	**Moderate/Medium**	**High**
Confidentiality *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*	The unauthorized disclosure of information could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets or individuals	The unauthorized disclosure of information could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have ***severe or catastrophic*** adverse effect on organizational operations, organization assets or individuals.
Integrity *Guarding against improper information modification or destruction, and includes insuring information non-repudiation and authenticity.*	The unauthorized modification or destruction of information could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets, or individuals	The unauthorized modification or destruction of information could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets, or individuals	The unauthorized modification or destruction of information could be expected to have a ***severe or catastrophic*** adverse effect on organizational operations, organizational assets, or individuals
Availability *Ensuring timely and reliable access to and use of information.*	The disruption of access to or use of information or an information system could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a ***severe or catastrophic*** adverse effect on organizational operations, organizational assets or individuals.

You do not have to include this table in the completed system security plan, it is provided here only as useful guidance.

Responsible Organization

- List organization responsible for the application

Information Contact(s)

- Name of person(s) knowledgeable about, or the owner of, the system. More than one point of contact may be provided.

Name:
Title:
Address:
Phone:
E-mail:

Assignment of Security Responsibility

- Name of person responsible for security of the system. More than one point of contact may be provided.

Name:
Title:
Address:
Phone:
E-mail:

System Operational Status

If more than one status is selected, list which part of the system is covered under each status.

- Operational
- Under Development
- Undergoing a major modification

General Description/Purpose

- Describe the function or purpose of the system and the information processed.
- Describe the processing flow of the application from system input to system output.
- List user organizations (internal & external) and type of data and processing provided.
- List all applications supported by the general support system. For each supported application, describe the functions and information processed.

System Environment

- Provide a general description of the technical system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.).
- Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.
- List any security software protecting the system and information.

System Interconnection/Information Sharing

- List interconnected systems and system identifiers (if appropriate).

- Provide the system name, organization, system type (major application or general support system.
- Indicate if there is an existing written authorization (MOUs, MOAs) on file, data of agreement to interconnect, information categorization, and name of authorizing personnel.

System Name	Organization	Type	Agreement (MOU/MOA)	Date	Information Categorization	Auth. Official

- It is ***necessary*** for systems requiring written authorizations (MOUs, MOAs) that they be obtained prior to connection with such systems and/or sharing sensitive data/information. Such an agreement (MOUs, MOAs) should detail the rules of behavior maintained by the interconnecting system owners. A description of these rules should be included with the security plan or discussed narratively in this section.
- If connected to an external system which does not have a security plan, provide a short discussion of any security concerns, which need to be considered for protection.

Applicable Laws or Regulations Affecting the System

- List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.

Minimum Security Controls (suggested)

- Use of guiding practice such as NIST 800-53 Rev 4 is suggested to help system owner understand the recommended baseline of security controls needed as informed by the information system categorization. Low-impact, Moderate-impact, and High-impact baselines are prescriptive when determining the minimum set of security controls for an application (inclusive of hardware and software).
- Security controls such as those suggested in the security control catalog of NIST SP 800-53 Rev 4, Appendix F, (http://dx.doi.org/10.6028/NIST.SP.800-53r4) have a well-defined organization and structure. Organized into classes and families for ease of use in the control selection and specification process; There are three general classes of security controls (i.e., management, operational, and technical). Each family contains security controls related to the security function of the family. A standardized, two-character identifier is assigned to uniquely identify each control family. The table below summarizes the classes and families in the security control catalog and the associated family identifiers.

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and	CA

	Security Assessments	
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Conclusion of Section 1 – General Information

The remainder of this major application security plan template is meant to be an assist for the application owner in documenting the Management, Operational and Technical controls, which will be utilized in securing the application, and the information intended to be housed and processed. Guiding text on the following pages of this template are suggestive and are not meant to be exhaustive, complete, or always applicable to each application. Only the informed application owner, with intimate business and organizational process asset knowledge and known state and federal applicable statutes, laws, and requirements can be expected to create a truly meaningful document.

2.0 MANAGEMENT CONTROLS

2.0 MANAGEMENT CONTROLS

Risk Assessment and Management

- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Include the date the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

Review of Security Controls

- List any independent security reviews conducted on the system in the last three years.
- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

Rules of Behavior

- A set of rules of behavior in writing must be established for each system. The rules of behavior should be made available to every user prior to receiving access to the system. It is recommended that the rules contain a signature page to acknowledge receipt.
- The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should state the consequences of inconsistent behavior or non-compliance. They should also include appropriate limits on interconnections to other systems.
- Attach the rules of behavior for the system as an appendix and reference the appendix number in this section or insert the rules into this section.

Planning for Security in the Life Cycle

Determine which phase(s) of the life cycle the system, or parts of the system are in. Describe how security has been handled in the life cycle phase(s) the system is currently in.

Initiation Phase

- Reference the sensitivity assessment, which is described in the NIST SP800-18, Section 3.7, *Sensitivity of Information Handled*.

Development/Acquisition Phase

- During the system design, were security requirements identified?
- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
- Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?
- Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

Implementation Phase

- Were design reviews and systems tests run prior to placing the system in production? Were the tests documented? Has the system been certified?
- Have security controls been added since development?
- Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?
- Include the date of the certification and accreditation. If the system is not authorized yet, include the date when the accreditation request will be made.

Operation/Maintenance Phase

- The security plan documents the security activities required in this phase.

Disposal Phase

- Describe in this section how information is moved to another system, archived, discarded, or destroyed. Discuss controls used to ensure the confidentiality of the information.
- Is sensitive data encrypted?
- How is information cleared and purged from the system?
- Is information or media purged, overwritten, degaussed or destroyed?

Authorize Processing

- Provide the date of authorization, name, and title of the management official authorizing processing in the system.
- If not authorized, provide the name and title of the manager requesting approval to operate, and the date of the request.

3.0 OPERATIONAL CONTROLS

3.0 OPERATIONAL CONTROLS

Personnel Security

- Have all positions been reviewed for sensitivity level?
- Have individuals received background screenings appropriate for the position to which they are assigned?
- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- Are critical functions divided among different individuals (separation of duties)?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?

Physical and Environmental Protection

- Discuss the physical protection for the system. Describe the area where processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.).
- Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems.

Production, Input/Output Controls

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to software should be listed. In this section, provide a synopsis of the procedures in place that support the system. Below is a sampling of topics that should be reported in this section.

- User Support - Is there a help desk or group that offers advice?
- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media
- Audit trails for receipt of sensitive inputs/outputs
- Procedures for restricting access to output products
- Procedures and controls used for transporting or mailing media or printed output
- Internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary)
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)
- Audit trails for inventory management
- Media storage vault or library-physical, environmental protection controls/procedures
- Procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing)
- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse
- Procedures for shredding or other destructive measures for hardcopy media when no

longer required

Contingency Planning

Briefly describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster were to occur. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix. Include descriptions for the following:

- Any agreements for backup processing
- Documented backup procedures including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)
- Location of stored backups and generations of backups kept
- Are tested contingency/disaster recovery plans in place? How often are they tested?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

Application Software Maintenance Controls

- Was the application software developed in-house or under contract?
- Does the government own the software? Was it received from another agency?
- Is the application software a copyrighted commercial off-the-shelf product or shareware? Has it been properly licensed and enough copies purchased for all systems?

- Is there a formal change control process in place and if so, does it require that all changes to the application software be tested and approved before being put into production?
- Are test data mirror of production data or obfuscated?
- Are all changes to the application software documented?
- Are test results documented?
- How are emergency fixes handled?
- Are there organizational policies against illegal use of copyrighted software, shareware?
- Are periodic audits conducted of users= computers to ensure only legal licensed copies of software are installed?
- What products and procedures are used to protect against illegal use of software?
- • Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?

Data Integrity Validation Controls

- Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
  - Are reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Are password crackers/checkers used?
- Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
- Are intrusion detection tools installed on the system?
- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?
- Is message authentication used in the application to ensure that the sender of a message is known and that the message has not been altered during transmission?

Documentation

Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security of the system to include backup and contingency activities, as well as descriptions of user and operator procedures.

- List the documentation maintained for the application (vendor documentation of hardware/software, functional requirements, security plan, general system security plan, application program manuals, test results documents, standard operating procedures, emergency procedures, contingency plans, user rules/procedures, risk assessment, certification/accreditation statements/documents, verification reviews/site inspections).

Security Awareness and Training

- Describe the awareness program for the application (posters, booklets, and trinkets).
- Describe the type and frequency of application training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training).
- Describe the procedures for assuring that employees and contractor personnel have been provided adequate training.

Incident Response Capability

- Are there procedures for reporting incidents handled either by system personnel or externally?
- Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?
- Who receives and responds to alerts/advisories, e.g., vendor patches, exploited vulnerabilities?
- What preventive measures are in place, i.e., intrusion detection tools, automated audit logs, penetration testing?

4.0 TECHNICAL CONTROLS

4.0 TECHNICAL CONTROLS

Identification and Authentication

- Describe the major application's authentication control mechanism(s).
- Describe the major application's method of user authentication (password, token, and biometrics).
- If a password system is used, provide the following specific information:
  - Allowable character set;
  - Password length (minimum, maximum);
  - Password aging time frames and enforcement approach;
  - Number of generations of expired passwords disallowed for use;
  - Procedures for password changes;
  - Procedures for handling lost passwords, and
  - Procedures for handling password compromise.
  - Procedures for training users and the materials covered.
  - Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).
- Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.
- Describe any token controls used on this system and how they are implemented.
- Describe the level of enforcement of the access control mechanism (network, operating system, and application).
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).
- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords).
- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.

- If digital signatures are used, the technology must conform with FIPS 186, *Digital Signature Standard* and FIPS 180-1, *Secure Hash Standard* issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures.

Logical Access Controls

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists (ACLs).
- How are access rights granted? Are privileges granted based on job function?
- Describe the system's capability to establish an ACL or register.
- Describe how users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent the user from accessing the system or applications outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.
- Indicate if encryption is used to prevent access to sensitive files as part of the system or application access control procedures.
- Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Dept. of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

Audit Trails

- Does the audit trail support accountability by providing a trace of user actions?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?
- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? (type of event, when the event occurred, user id associated with the event, program or command used to initiate the event.)
- Is access to online audit logs strictly enforced?
- Is the confidentiality of audit trail information protected if, for example, it records personal information about users?
- Describe how frequently audit trails are reviewed and whether there are guidelines.

- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?