SECURITY PLAN TEMPLATE
For Major Applications
and General Support Systems

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A. APPLICATION/SYSTEM IDENTIFICATION

A.1 Application/System Category

- Indicate whether the application/system is a Major Application or a General Support System.
- A Major Application is "an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application."
- A General Support System is an "interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people."

A.2 Application/System Name/Title

- Unique identifier & name given to the application/system

A.3 Responsible Organization

- Organization responsible for the application/system

A.4 Information Contact(s)

- The owner(s) of the application/system and at least one other manager expertly knowledgeable about it.

-- Name
-- Title
-- Address
-- Phone Number
-- Fax Number
-- E-mail Address

A.5 Assignment of Security Responsibility

- Person(s) responsible for security of the application/system and an alternate emergency contact.

-- Name
-- Title
-- Address
-- Phone Number
-- Fax Number
-- E-mail Address

- Describe roles and responsibilities of all users having access to the application/system. Include approximate number of authorized users and their physical location.

A.6 Application/System Operational Status

- If more than one status is selected, list which part(s) of the application/system are covered under each status.

-- Operational
-- Under Development
-- Undergoing a major modification

A.7 General Description/Purpose

- Describe the function or purpose of the application/system and the information processed.
- Describe the processing flow of the application/system from input to output.
- List user organizations (internal & external) and the type of data and processing provided.

A.8 Application/System Environment

- Provide a general description of the technical application/system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.) Include a diagram of architecture here or in an appendix, if applicable.
- Describe the primary computing platform(s) used and a description of the principal application/system components, including hardware, software, and communications resources.
- Include any security software protecting the application/system and information.
- List the physical location(s) of the application/system.

A.9 Application/System Interconnection/Information Sharing

The NIST Guide strongly recommends that written authorization, such as a memorandum of understanding (MOU) or a memorandum of agreement (MOA), be obtained prior to connection with other applications/systems and/or sharing sensitive data/information. This section should list any such agreements. The written authorization should detail the rules of behavior and controls that must be maintained by the interconnecting systems.

- List interconnected applications/systems and application/system identifiers (if appropriate).
- If connected to an external application/system not covered by a security plan, provide a brief discussion of any security concerns that need to be considered for protection.
- A description of the rules for interconnecting applications/systems and for protecting shared data must be included with this security plan.

A.10 Applicable Laws or Regulations Affecting the Application/System

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

A.11 Information Sensitivity and Criticality Assessment

All applications/systems require protection for confidentiality, integrity, and availability. The level of protection required is determined by an evaluation of the sensitivity and criticality of the information processed; the relationship of the application/system to the organization's mission, and the economic value of the application/system components.

The sensitivity and criticality of the information stored within, processed by, or transmitted by an application/system provides a basis for the value of the application/system and is one of the major factors in risk management. A description of the types of information handled by the application/system and an analysis of the criticality of the information is required. This description and analysis will assist in designing security controls, facilitating security audits, and implementing security countermeasures.

- Describe, in general terms, the information handled by the application/system and the need for protective measures.
- List the types of sensitive information the application/system accesses. Examples may include: administrative, financial, grant/contract, patient, proprietary, research, Privacy Act.
- Relate the information processed to each of the three basic protection requirements.

-- **Confidentiality** refers to information that requires protection from unauthorized disclosure.
-- **Integrity** refers to information that must be protected from unauthorized, unanticipated, or unintentional modification.
-- **Availability** refers to information or services that must be available on a timely basis to meet mission requirements.

- For each of the three protection requirements above (confidentiality, integrity, and availability), indicate if the sensitivity is classified as: **High, Medium, or Low**.

-- **Low Sensitivity** information requires a minimal amount of protection. This level includes information considered to be in the public domain.
-- **Medium Sensitivity** includes data important to NIH that must be protected from unauthorized alteration. This level includes information pertaining to correspondence and other document files whose release needs to be controlled.
-- **High Sensitivity** information requires the greatest safeguards at the user level. High sensitivity information includes but is not limited to: highly critical or proprietary information; financial or grant data; or records subject to the Privacy Act.

SAMPLE APPLICATION/SYSTEM PROTECTION REQUIREMENTS CHART

Application/System Protection Requirements	**High**	**Medium**	**Low**
Confidentiality			
Integrity			
Availability			

- A more detailed chart may be used if the application/system processes information with different levels of application/system protection requirements.

SAMPLE DETAILED APPLICATION/SYSTEM PROTECTION REQUIREMENTS CHART

Information Type	**Confidentiality (High, Medium or Low)**	**Integrity**	**Availability**
Administrative			
Financial			
Grant/Contract			
Patient			
Proprietary			

Research			
Privacy Act			
Other (specify)			

- 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 application/system.

B. MANAGEMENT CONTROLS

B.1 Risk Assessment and Management

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

B.2 Review of Security Controls

- List any independent security reviews conducted on the application/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.

B.3 Rules of Behavior

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

B.4 Planning for Security in the Life Cycle

Although a computer security plan can be developed for an application/system at any point in the life cycle, the recommended approach is to design the plan at the beginning of the computer system life cycle. It is recognized that in some cases, at any one time the application/system may be in several phases of the life cycle. For example, a large human resources system may be in the operation/maintenance phase, while an older, batch-oriented input sub-system is being replaced by a new, distributed, interactive user interface. In this case, the life cycle phases for the application/system include the disposal phase (data and equipment) related to the retirement of the batch-oriented transaction system, the initiation and acquisition phase associated with the replacement interactive input system, and the operations/maintenance phase for the balance of the application/system.

In this section, determine which phase(s) of the life cycle the application/system, or parts of the application/system, are in. Identify how security has been handled during each of the listed applicable life cycle phases.

- Initiation
- Development/Acquisition
- Implementation
- Operation/Maintenance
- Disposal

B.5 Authorization to Process

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

C. OPERATIONAL CONTROLS

C.1 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?

C.2 Physical and Environmental Protection

- Discuss the physical protection in the area where application/system 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.

C.3 Production, Input/Output Controls

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

- Is there a help desk or group that offers advice and can respond to security incidents in a timely manner? Are there procedures in place documenting how to recognize, handle, report, and track incidents and/or problems? Do these procedures outline how to categorize and prioritize incidents?
- Are there procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
- Are there procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media?
- Are there audit trails for receipt of sensitive inputs/outputs?
- Are there procedures for restricting access to output products?
- Is there internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary?)
- Is there external labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)?
- Are there audit trails for inventory management?
- Is there a media storage vault or library containing physical, environmental protection controls/procedures?
- Are there procedures for sanitizing electronic media for reuse?
- Are there procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse?
- Are there procedures for shredding or other destructive measures for hardcopy media when no longer required?

C.4 Contingency Planning

- Briefly describe the procedures (contingency plan) that would be followed to ensure the application/system continues to be processed if the supporting IT application/system were unavailable. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan may be attached as an appendix. Include descriptions for the following:

-- Agreements of 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

- 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?
- Coverage of backup procedures, e.g., what is being backed up?

C.5 Application/System Hardware and Software Maintenance Controls

- Are there restrictions/controls on those who perform hardware and software maintenance and repair activities?
- Are there special procedures for performance of emergency repair and maintenance?
- Are there procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site)?
- Are there procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements?
- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?
- Was the application/system software developed in-house or under contract?
- Does the government own the software? Was it received from another agency?
- Is the application/system software a copyrighted commercial off-the-shelf product or shareware?
- Has the software been properly licensed, and have enough copies been purchased for the application/system?
- Are there organizational policies against illegal use of copyrighted software and shareware?
- Are periodic audits conducted of users' computers to ensure that only legal licensed copies of software are installed?
- What products and procedures are used to protect against illegal use of software?
- Describe any formal change control process in place.

-- Is there version control that allows association of application/system components to the appropriate application/system version?
-- Are all changes to the application/system software or application/system components documented?
-- Are there impact analyses to determine the effect of proposed changes on existing security control to include the required training for both technical and user communities associated with the change in hardware/software?
-- Are there change identification, approval, and documentation procedures?
-- Are there procedures for ensuring contingency plans and other associated documentation are updated to reflect application/system changes?

- Does the change control process require that all changes to the application/system software be tested and approved before being put into production?
- Are there procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production?
- Is test data live data or made-up data?
- Do test plans trace back to the original security requirements?
- Are test results documented?

C.6 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 application/system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Are integrity verification programs used by the application/system to look for evidence of data tampering, errors, and omissions?
- Is an intrusion detection tool installed to monitor the application/system?
- Are procedures in place to handle and close out security incidents?
- Are other network security software packages used?
- Is application/system performance monitoring used to analyze performance logs in real time to look for availability problems, including active attacks, and application/system and network slowdowns and crashes?
- Is penetration testing performed on the application/system? If so, what procedures are in place to ensure that tests are conducted appropriately?
- Is message authentication used in the application/system to ensure that the sender of a message is known and that the message has not been altered during transmission?

C.7 Documentation

Documentation includes descriptions of the hardware and software, policies, procedures, and approvals related to automated information security in the application/system. Documentation should also include descriptions of user and operator procedures, and backup and contingency activities.

- List the documentation maintained for the application/system. Examples may include:

-- vendor documentation of hardware/software
-- functional requirements
-- design specifications
-- source code documents
-- testing procedures and results
-- records of verification reviews/site inspections
-- standard operating procedures
-- user rules/manuals
-- emergency procedures
-- contingency plans
-- risk assessments

- Describe the procedure used to update documentation.
- List the physical location of documentation.

C.8 Security Awareness and Training

- Describe the type and frequency of application/system-specific training provided to employees and contractor personnel (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.
- Describe the awareness program for the application/system.

C.9 Incident Response Capability

- Are there procedures for reporting incidents handled either by application/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 preventative measures are in place, i.e., intrusion detection tools, automated audit logs, penetration testing?

D. TECHNICAL CONTROLS

D.1 Identification and Authentication

- Describe the application/system's user authentication control mechanisms (password, token, and biometrics).
- Indicate the frequency of password changes, describe how changes are enforced, and identify who changes the passwords (the user, the system administrator, or the application/system).
- Provide the following if an additional password system is used in the application/system:

-- password length (minimum, maximum)
-- allowable character set
-- password aging time frames and enforcement approach
-- number of generations of expired passwords disallowed for use
-- procedures for password changes (after expiration and forgotten/lost)
-- procedures for handling password compromise
-- procedures for training users and the materials covered

- Describe the level of enforcement of the access control mechanism (network, operating system, and application/system).
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords associated with a user ID that is assigned to a single person).
- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords encrypted while in transmission, automatically generated, or checked against a dictionary of disallowed passwords).
- State the number of invalid access attempts that may occur for a given user ID or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all application/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 application/systems).
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifiers, and group user identifiers) and any compensating controls.
- Describe any use of digital or electronic signatures and the standards used. Discuss the management procedures for key generation, distribution, storage, and disposal. 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.

D.2 Logical Access Controls

Discuss the controls in place to authorize or restrict the activities of users and personnel within the application/system. Describe hardware or software features that are designed to permit only authorized access to or within the application/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 application/system's capability to establish an ACL or register.
- Describe how users are restricted from accessing the operating system or other application/system resources not required in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent users from accessing the application/system outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the application/system automatically blanks associated display screens and/or disconnects inactive users. After what period of user inactivity does the application/system require the user to enter a unique password before reconnecting?
- Indicate if encryption is used to prevent access to sensitive files as part of the application/system access control procedures.
- Describe the rationale for electing to use or not use warning banners, and provide an example if banners are used.

D.3 Public Access Controls

- If the public accesses the application/system, discuss the additional security controls used to protect the application/system's integrity. What additional controls are used to protect the confidence of the public in the application/system? Such controls include segregating information made directly accessible to the public from official agency records. Others may include:

-- Some form of identification and authentication
-- Access controls to limit what the user can read, write, modify, or delete
-- Controls to prevent public users from modifying information in the application/system
-- Digital signatures
-- CD-ROM for on-line storage of information for distribution
-- Copies of information for public access available on a separate application/system

-- Controls to prohibit the public from accessing live databases
-- Verification that programs and information distributed to the public are virus-free
-- Audit trails and user confidentiality
-- Application/system and data availability
-- Legal considerations

D.4 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 and remediation? Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them (e.g., 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 it records personal user information?
- Describe how frequently audit trails are reviewed and whether guidelines exist.
- Does the appropriate application/system level administrator review audit trails following a known application/system software problem, an unexplained application/system or user problem, or a known violation of existing requirements by a user?

Appendix A
Sample Authorization to Process (ATP) Memo

MEMORANDUM

DATE:

TO: Senior Information Systems Security Officer (ISSO)

FROM: Application/System XYZ Owner

SUBJECT: Security Authorization for Application/System XYZ

Based on a careful review of the Application System XYZ Security Plan, I have confirmed that Application/System XYZ meets the requirements of ______________________information systems security programs. Therefore, I authorize continued operation of Application/System XYZ under the following restrictions:

[List any restrictions here, or write "None."]

I further authorize initiation of the following corrective actions, scheduled to be completed by the dates listed below:

[List any corrective actions here, or write "None."]

Owner of Application/System XYZ

[Name] ____

[Title] ____

Signature ____

Person responsible for security of Application/System XYZ

[Name] ____

[Title] ____

Signature ____