Information Technology Security Management Plan

[Contract Name]

[Contract Number]

Issue Date: Click here to enter a date.

Effective Date: Click here to enter a date.

Change History

Version	Date	Change Description
1.0	MM/DD/YYYY	Initial Contract Name IT Security Management Plan
	MM/DD/YYYY	
	MM/DD/YYYY	
	MM/DD/YYYY	
	MM/DD/YYYY	
	MM/DD/YYYY	
	MM/DD/YYYY	
	MM/DD/YYYY	
	MM/DD/YYYY	
	MM/DD/YYYY	

IT Security Management Plan Review and Approval

This Information Technology Security Management Plan (ITSMP) for the [Contract Name] was prepared for the exclusive use of NASA and completed on Click here to enter a date.

I have reviewed the contents of this plan, and believe that it presents an accurate representation.

Reviewed by: _____ Click here to enter a date.

ISSO, or equivalent Date

Concurred by: _____ Click here to enter a date.

COR/Task Monitor Date

Approved by: _____ Click here to enter a date.

Center CISO Date

Accepted by: _____ Click here to enter a date.

Contracting Officer Date

Contents

Change History ii
IT Security Management Plan Review and Approval iii
1 Contract Identification 1
1.1 Contract Name 1
1.2 Contract Number 1
1.3 Responsible Organization 1
1.4 Contact Information 1
1.4.1 Physical Location 1
1.4.2 Points of Contact 1
1.5 General Contract Description 2
1.5.1 Information System Categorization 2
1.5.2 Security Categorization 2
1.5.3 Information System 3
1.5.4 Contractor Badging 3
1.5.5 Related Laws/Regulations/Policies 3
2 Security Control Implementations 5
Appendix A: Acronyms 11

1 Contract Identification

1.1 Contract Name

Contract Name: Contract Name

Contract Abbreviation:

1.2 Contract Number

Contract Number: Contract Number

1.3 Responsible Organization

The overarching responsible organization is NASA. The responsible organization can be the associated mission directorate, Center, division, etc.

National Aeronautics and Space Administration (NASA)

Responsible Organization:

1.4 Contact Information

1.4.1 Physical Location

Include the physical location where NASA data resides and/or where contact with NASA data occurs. Depending on the contract and/or information systems, there may be multiple physical locations.

Location Name	Street Address	City	State	Zip Code	Country

1.4.2 Points of Contact

.

Title	Name	Telephone	Email Address
Contracting Officer (CO)			
Contracting Officer Representative (COR)			
Contractor Representative			

1.5 General Contract Description

Purpose/Function *Include a brief description of the purpose/function of the contract.*	

1.5.1 Information System Categorization[1]

List all information types stored, processed or transmitted in performance of the contract.

Additional rows may be added as needed.

Information Type	Confidentiality Impact Level (L/M/H)	Integrity Impact Level (L/M/H)	Integrity Impact Level (L/M/H)

1.5.2 Security Categorization

Based on the information provided in section 1.5.1, the security impact levels for each of the three security objectives of confidentiality, integrity, and availability are identified below.

Security Objective	Security Impact Level (L/M/H)
Confidentiality:	**<FIPS 199 CONFIDENTIALITY IMPACT LEVEL>**
Integrity:	**<FIPS 199 INTEGRITY IMPACT LEVEL>**
Availability:	**<FIPS 199 AVAILABILITY IMPACT LEVEL>**

Table: Security Objectives Impact

Based on the information provided in the Security Objectives Impact table above, the required protection level for Agency Common Controls has been identified and is reflected in the following System High Water Mark table. The high water mark represents the minimum level of security controls appropriate for the system.

[1] Please use NIST SP 800-60 to identify the information types and the confidentiality, integrity and availability impact levels.

High Water Mark	<FIPS 199 High Water Mark>

Table: System High Water Mark

1.5.3 Information System

Indicate whether the contract provides or manages an external information system to process NASA data.

☐	**The contract provides or manages an external information system to store or process NASA data.**
If this box is checked, the system requires an Authorization to Process/Store (ATP/S) NASA information. The contract representative should work with the Center Assessment and Authorization Official to obtain a system unique identifier and the Contracting Officer's Technical Representative (COTR) to initiate the Assessment and Authorization (A&A) process (reference ITS-HBK 2810.02-05A Security Assessment and Authorization: External Information Systems).	
☐	**The contract does not provide or manage an external information system to store or process NASA data.**
If this box is checked, the contract is not responsible for an external information system security plan; therefore, the ITSMP is sufficient to describe the security processes and procedures that will be followed by the contract.	
☐	**All information technology components used in the performance of the contract are managed under an internal NASA information system.**
If this box is checked, the contract is not responsible for an external information system security plan, however, the contractor is responsible for identifying the NASA information system under which the contract is performed. NASA Information System Name: NASA Information System Number:	

1.5.4 Contractor Badging

Indicate whether or not contractor personnel will be issued NASA badges.

☐	**Contractor personnel will be NASA badged.**
If this box is checked, contractors, by virtue of being NASA badged, will automatically fall under many NASA policies and procedures. Consideration of the above should influence the completion of Section 2 of this document.	
☐	**Contractor personnel will not be NASA badged.**
If this box is checked, the contract may not be able to leverage many of NASA's policies and procedures. If so, provide details in Section 2 that meet the general intent of the control descriptions.	

1.5.5 Related Laws/Regulations/Policies

- 5 U.S.C. 552, Freedom of Information Act, 1967
- 5 U.S.C. 552a, Privacy Act, 1974
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-30, Risk Management Guide for Information Technology Systems
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems
- NIST SP 800-37, Guide for the Security Authorization of Federal Information Systems
- NIST SP 800-42, Guideline on Network Security Testing
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- NIST SP 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems

- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-61, Computer Security Incident Handling Guide
- NIST SP 800-64, Security Considerations in the Information System Development Life Cycle
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- Public Law (PL) 99-474, The Computer Fraud and Abuse Act of 1986
- PL 93-502 -Freedom of Information Act 1974
- Presidential Decision Directive (PDD-63), Critical Infrastructure Protection Federal Information Security Management Act of 2002 (FISMA)
- NPR 2810.1, Security of Information Technology

2 Security Control Implementations

In completing control detail, the author should explain how the contract meets the intent of the control description. In some cases, implementation detail is already included. The author may accept the pre-populated language as is, add to it, modify it, or overwrite it. Note that if the "Contractor will be NASA-badged" is selected in Section 1.5.2, then the author should explore accepting relevant NASA-provided implementation detail. If the author believes that the control is not applicable to their contract, the "Not Applicable to System/Contract" box should be checked and a short explanation as to why it is not applicable should be included.

Briefly describe the Justification/Implementation Detail; this description should allow a reviewer to have a basic understanding of the implementation. If contractor personnel will be NASA badged, references to appropriate NASA policies and procedures are sufficient. See Contract Attachment entitled, IT Security Applicable Documents List" for relevant NASA policies and procedures.

Planning relates to the definition and documentation of the key resources and activities used to protect information and information systems. Effective security planning is both comprehensive and flexible.

(ITS-HBK-2810.03-01, ITS-HBK-2810.03-02)

PL-4: Rules of Behavior

Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		NASA IT Rules of Behavior are fully detailed in the SATERN IT Security awareness training module, which covers the appropriate use of government resources, password security, software usage, user responsibilities, and encryption requirement for sensitive data. All employees that handle NASA data are required to take this training annually. As part of the continuous monitoring workbook a signed acknowledgment from users indicating that they understand, and agree to abide by the rules of behavior is provided annually to the Center CISO. *The SATERN IT Security awareness training module, via CD, will be obtained annually from the Center CISO or the NASA IT Security Awareness & Training Center (ITSATC).* System- or contract-specific detail is provided below.
The organization: *a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and* *b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.*		

Security Awareness and Training relates to the information security knowledge requirements for all users of information systems, and the development and delivery of courses and other training resources to enable and validate satisfaction of those requirements. Users are responsible for meeting Agency security training requirements in order to gain and maintain access to any NASA information system resource.

Furthermore, certain roles, including managers and those with significant information security responsibilities, have to comply with additional security training and awareness requirements.

(ITS-HBK-2810.06-01)

AT-1: Security Awareness and Training Policy and Procedures

Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		In accordance with the NASA FAR, external systems are subject to the requirements of NPR 2810 and applicable requirements, regulations, policies, and guidelines are identified in the Applicable Documents List (ADL). If applicable, additional organizational or contract-specific policies should be referenced here.
The organization develops, disseminates, and reviews/updates [Assignment: organization define frequency]: *a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and* *b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.*		

AT-2: Security Awareness

Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		The SATERN IT Security awareness training module, via CD, will be obtained

The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [Assignment: organization-defined frequency] thereafter.	annually from the Center CISO or the NASA IT Security Awareness & Training Center (ITSATC). All employees that handle NASA data are required to take this training annually. *The SATERN IT Security awareness training module, via CD, will be obtained annually from the Center CISO or the NASA IT Security Awareness & Training Center (ITSATC).* If applicable, system- or contract-specific detail is provided below.

AT-3: Security Training		
Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.
The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.		

Incident Response relates to dealing with the potential for and actual damage and disruption to information systems. An "incident" is any adverse event or situation associated with a system that poses a threat to the system's integrity, availability, or confidentiality. An incident may result in or stem from any one of the following: a failure of security controls; an attempted or actual compromise of information; and/or waste, fraud, abuse, loss, or damage of government property or information.

(ITS-HBK-2810.09-01)

IR-6: Incident Reporting		
Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		All breaches will be communicated to the [Center] CISO and the NASA SOC within the timeframe appropriate to the category of information involved. If there is PII involved in the breach the SOC will be contacted with one hour. • The SOC may be contacted at 877-NASA SEC (877-627-2732). • The Center CISO and/or the OIG handles the notification to external authorities. If applicable, system- or contract-specific detail is provided below.
The organization: *a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time-period]; and* *b. Reports security incident information to designated authorities.*		

Media Protection relates to the secure use of information storage media. Storage media can take one of two forms – digital or non-digital. Non-digital media typically consists of paper, film, microfilm, microfiche, etc. Digital media is comprised of mobile computing devices, laptops, PDAs, "smart phones," and removable storage devices such as USB drives, flash drives, writeable CDs and DVDs, memory cards, external hard drives, storage cards, diskettes, magnetic tapes or any electronic device that can be used to copy, save, store and/or move data from one system to another.

(ITS-HBK-2810.11-01, ITS-HBK-2810.11-02)

MP-1: Media Protection Policy and Procedures		
Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		In accordance with the NASA FAR, external systems are subject to the requirements of NPR 2810 and applicable requirements, regulations, policies, and guidelines are identified in the Applicable Documents List (ADL). If applicable, system- or contract-specific policies should be referenced here.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and* *b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.*		

MP-3: Media Marking		
Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.

The organization: *a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and* *b. Exempts [Assignment: organization-defined list of removable media types] from marking as long as the exempted items remain within [Assignment: organization-defined controlled areas].*	
MP-4: Media Storage	
Not Applicable to System/Contract ☐	Justification/Implementation Detail
Control Description	System- or contract-specific detail is provided below.
The organization: *a. Physically controls and securely stores [Assignment: organization-defined types of digital and non-digital media] within [Assignment: organization-defined controlled areas] using [Assignment: organization-defined security measures];* *b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.*	
MP-5: Media Transport	
Not Applicable to System/Contract ☐	Justification/Implementation Detail
Control Description	System- or contract-specific detail is provided below.
The organization: *a. Protects and controls [Assignment: organization-defined types of digital and non-digital media] during transport outside of controlled areas using [Assignment: organization-defined security measures];* *b. Maintains accountability for information system media during transport outside of controlled areas; and* *c. Restricts the activities associated with transport of such media to authorized personnel.*	
MP-6: Media Sanitization	
Not Applicable to System/Contract ☐	Justification/Implementation Detail
Control Description	System- or contract-specific detail is provided below.
The organization: *a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and* *b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.*	
Configuration Management relates to the organizational aspects of information system baseline configurations, establishing review and validation, and change control. It also manages administrator roles, and the ability of individuals to make changes to the information systems' configuration. (ITS-HBK-2810.07-01, ITS-HBK-2810.02-04)	
CM-8: Information System Component Inventory	
Not Applicable to System/Contract ☐	Justification/Implementation Detail
Control Description	System- or contract-specific detail is provided below.
The organization develops, documents, and maintains an inventory of information system components that: *a. Accurately reflects the current information system;* *b. Is consistent with the authorization boundary of the information system;* *c. Is at the level of granularity deemed necessary for tracking and reporting;* *d. Includes [Assignment: organization-defined information deemed necessary to achieve effective property accountability]; and* *e. Is available for review and audit by designated organizational officials.*	
Physical and Environmental Protection relates to the activities and requirements surrounding the development, implementation, and maintenance of physical access authorizations and controls (e.g., key and security badge distribution, visitor management, and related record keeping), and the protection, proofing, and regulation of facilities. This section also addresses protection of facilities and the essential utilities and infrastructure which support those facilities (e.g., door locks, backup power and lighting, emergency plumbing shutoff switches, and fire suppression systems), and environmental controls for those facilities (e.g., temperature regulation, humidity	

monitoring), as appropriate.

(ITS-HBK-2810.12-01)

PE-3: Physical Access Control

Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.
The organization: *a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);* *b. Verifies individual access authorizations before granting access to the facility;* *c. Controls entry to the facility containing the information system using physical access devices and/or guards;* *a. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;* *b. Secures keys, combinations, and other physical access devices;* *c. Inventories physical access devices [Assignment: organization-defined frequency]; and* *d. Changes combinations and keys [Assignment: organization-defined frequency] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.*		

Personnel Security relates to the security activities that surround various facets of the employment life cycle (i.e., initial employee screening, position categorization, authority delegation, sanctioning, transfers, and termination). Personnel Security applies to both direct employees of the Agency as well as contracted personnel, and service bureaus.

(ITS-HBK-2810.13-01)

PS-2: Position Categorization

Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.
The organization: *a. Assigns a risk designation to all positions;* *b. Establishes screening criteria for individuals filling those positions; and* *c. Reviews and revises position risk designations [Assignment: organization-defined frequency].*		

PS-3: Personnel Screening

Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.
The organization: *a. Screens individuals prior to authorizing access to the information system; and* *b. Rescreens individuals according to [Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening].*		

PS-4: Personnel Termination

Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.
The organization, upon termination of individual employment: *a. Terminates information system access;* *b. Conducts exit interviews;* *c. Retrieves all security-related organizational information system-related property; and* *d. Retains access to organizational information and information systems formerly controlled by terminated individual.*		

PS-7: Third-Party Personnel Security

Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.

The organization: *a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;* *b. Documents personnel security requirements; and* *c. Monitors provider compliance.*	

PS-8: Personnel Sanctions		
Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.
The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.		

Access Control relates to the ability to permit or deny access to computer systems, system locations and system information based on a user's need to know. It encompasses the management of unique account identifiers (IDs), passwords, physical access, badges and tokens, and user permissions to ensure the proper level of system access.

(ITS-HBK-2810.15-01, ITS-HBK-2810.15-02A)

AC-2: Account Management		
Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.
The organization manages information system accounts, including: *a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);* *b. Establishing conditions for group membership;* *c. Identifying authorized users of the information system and specifying access privileges;* *d. Requiring appropriate approvals for requests to establish accounts;* *e. Establishing, activating, modifying, disabling, and removing accounts;* *f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;* *g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;* *h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;* *i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and* *j. Reviewing accounts [Assignment: organization-defined frequency].*		

AC-5: Separation of Duties		
Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.
The organization: *a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;* *b. Documents separation of duties; and* *c. Implements separation of duties through assigned information system access authorizations.*		

AC-6: Least Privilege		
Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.
The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.		

AC-20: Use of External Information Systems		
Not Applicable to System/Contract	☐	Justification/Implementation Detail
Control Description		System- or contract-specific detail is provided below.
The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: *a. Access the information system from the external information systems; and* *b. Process, store, and/or transmit organization-controlled information using the external information systems.*		

Appendix A: Acronyms

Acronym	Definition
ADL	Applicable Documents List
CISO	Chief Information Security Officer
CO	Contracting Officer
COR	Contracting Officer Representative
FIPS	Federal Information Processing Standards
ISSO	Information System Security Officer
ITSATC	IT Security Awareness & Training Center
NIST-SP	National Institute of Standards and Technology – Special Publications
NPR	NASA Procedural Requirements
SOC	Security Operations Center