NASA Information Technology Security Management Plan

Contract Name

Prepared For:

National Aeronautics and Space Administration

300 E St., SW
Washington D.C. 20546

WHEN COMPLETED, THIS ATTACHED MATERIAL MAY CONTAIN NASA INFORMATION THAT IS "FOR OFFICIAL USE ONLY," OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS THEN MUST BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH NASA MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND, WHEN UNATTENDED, MUST BE STORED IN A LOCKED CONTAINED OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.

Preface

To carry out its wide-ranging responsibilities, the National Aeronautics and Space Administration (NASA), and its employees and managers have access to diverse and complex automated information systems, which include file servers, local and wide area networks running on various platforms, and telecommunications systems to include communications equipment. The offices within NASA depend on the confidentiality, integrity, and availability of these systems and their data in order to accomplish day-to-day activities.

Title 48: Federal Acquisition Regulations System, Section 1852.204-76 outlines the security requirements for unclassified information technology resources. IT Security Management Plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. Unlike the IT security plan, which addresses the IT system, the IT Security Management Plan addresses how the contractor will manage personnel and processes associated with IT Security on the instant contract.

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: _____ **Date**: Click here to enter a date.

Contractor Manager

Contents

Preface i
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 Related Documents 2
2 Security Control Implementations 3
2.1 Management Controls 3
2.2 Operational Controls 3
2.3 Technical Controls 5
Appendix A: Acronyms 7

1 Contract Identification

1.1 Contract Name

Please include the 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 of the information system. Depending on the information system, 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) *The CO is the NASA procurement official responsible for the initial award and set-up of the contract.*			
Contract Manager *The Contract Manager is the contractor point of contact for general program management of the contract,*			

1.5 General Contract Description

Include language here regarding the systems and interconnections that the contract involves. Also include whether contractors will be badged, and whether the contract utilizes an infrastructure external to NASA.

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

1.5.1 Related Documents

- 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, Guide for Conducting Risk Assessments
- NIST SP 800-34, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
- 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

The security controls, as described by *NIST SP 800-53*, which relate directly to the general management and overall security approach of the contract are addressed in the following sections.

2.1 Management Controls

Briefly describe the justification/Implementation Detail, this description should allow a reviewer to have a basic understanding of the implementation.

CA-1: Security Assessment and Authorization Policies and Procedures		
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and* *a. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.*		

PL-1: Security Planning Policy and Procedures		
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented security planning 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 planning policy and associated security planning controls.*		

RA-1: Risk Assessment Policy and Procedures		
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented risk assessment 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 risk assessment policy and associated risk assessment controls.*		

SA-1: System and Services Acquisition Policy and Procedures		**CAG 3 – Secure Configurations for Hardware and Software**
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented system and services acquisition policy that includes information security considerations and 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 system and services acquisition policy and associated system and services acquisition controls.*		

2.2 Operational Controls

Briefly describe the justification/Implementation Detail, this description should allow a reviewer to have a basic understanding of the implementation.

AT-1: Security Awareness and Training Policy and Procedures		**CAG 20 – Security Skills Assessment and Appropriate Training to Fill Gaps**
Not Applicable to System	☐	Justification/Implementation Detail
Control Description		

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.*	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.

CM-1: Configuration Management Policy and Procedures	**CAG 2 – Inventory of Authorized and Unauthorized Software** **CAG 3 – Secure Configurations for Hardware and Software** **CAG 4 – Secure Configurations for Network Devices**
Not Applicable to System ☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented configuration management 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 configuration management policy and associated configuration management controls.*	

CP-1: Contingency Planning Policy and Procedures	
Not Applicable to System ☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented contingency planning 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 contingency planning policy and associated contingency planning controls.*	

IR-1: Incident Response Policy and Procedures	**CAG 18 – Incident Response Capability**
Not Applicable to System ☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented incident response 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 incident response policy and associated incident response controls.*	

MA-1: System Maintenance Policy and Procedures	
Not Applicable to System ☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented information system maintenance 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 information system maintenance policy and associated system maintenance controls.*	

MP-1: Media Protection Policy and Procedures	
Not Applicable to System ☐	Justification/Implementation Detail
Control Description	

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.*	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.

PE-1: Physical and Environmental Protection Policy and Procedures		
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented physical and environmental 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 physical and environmental protection policy and associated physical and environmental protection controls.*		

PS-1: Personnel Security Policy and Procedures		
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented personnel security 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 personnel security policy and associated personnel security controls.*		

SI-1: System and Information Integrity Policy and Procedures		
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented system and information integrity 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 system and information integrity policy and associated system and information integrity controls.*		

2.3 Technical Controls

Briefly describe the justification/Implementation Detail, this description should allow a reviewer to have a basic understanding of the implementation.

AC-1: Access Control Policy and Procedures		**CAG 9 – Controlled Access Based on Need to Know**
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented access control 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 access control policy and associated access controls.*		

AU-1: Audit and Accountability Policy and Procedures		
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented audit and accountability 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 audit and accountability policy and associated audit and accountability controls.*		

IA-1: Identification and Authentication Policy and Procedures		
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented identification and authentication 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 identification and authentication policy and associated identification and authentication controls.*		

SC-1: System and Communications Protection Policy and Procedures		
Not Applicable to System	☐	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). The documents listed in the ADL are found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html. If there are variances to the NPR in the external system policy they are listed below.
The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]: *a. A formal, documented system and communications 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 system and communications protection policy and associated system and communications protection controls.*		

Appendix A: Acronyms

Acronym	Definition
ADL	Applicable Documents List
NPR	NASA Procedural Requirements
SBU	Sensitive But Unclassified