<PROJECT NAME>

SECURITY APPROACH

Version Number: <1.0>

Version Date: <mm/dd/yyyy>

Notes to the Author

[This document is a template of a Security Approach document for a project. The template includes instructions to the author, boilerplate text, and fields that should be replaced with the values specific to the project.

- *Blue italicized text enclosed in square brackets ([text]) provides instructions to the document author, or describes the intent, assumptions and context for content included in this document.*
- *Blue italicized text enclosed in angle brackets (<text>) indicates a field that should be replaced with information specific to a particular project.*
- *Text and tables in black are provided as boilerplate examples of wording and formats that may be used or modified as appropriate to a specific project. These are offered only as suggestions to assist in developing project documents; they are not mandatory formats.*

When using this template, the following steps are recommended:

1. *Replace all text enclosed in angle brackets (e.g., <Project Name>) with the correct field document values. These angle brackets appear in both the body of the document and in headers and footers. To customize fields in Microsoft Word (which display a gray background when selected) select File->Properties->Summary and fill in the appropriate fields within the Summary and Custom tabs.*

   After clicking OK to close the dialog box, update all fields throughout the document selecting Edit>Select All (or Ctrl-A) and pressing F9. Or you can update each field individually by clicking on it and pressing F9.

   These actions must be done separately for any fields contained with the document's Header and Footer.
2. *Modify boilerplate text as appropriate for the specific project.*
3. *To add any new sections to the document, ensure that the appropriate header and body text styles are maintained. Styles used for the Section Headings are Heading 1, Heading 2 and Heading 3. Style used for boilerplate text is Body Text.*
4. *To update the Table of Contents, right-click on it and select "Update field" and choose the option - "Update entire table".*
5. *Before submission of the first draft of this document, delete this instruction section "Notes to the Author" and all instructions to the author throughout the entire document.*

VERSION HISTORY

[Provide information on how the development and distribution of the Security Approach will be controlled and tracked. Use the table below to provide the version number, the author implementing the version, the date of the version, the name of the person approving the version, the date that particular version was approved, and a brief description of the reason for creating the revised version.]

Version Number	Implemented By	Revision Date	Approved By	Approval Date	Description of Change
1.0	*<Author name>*	*<mm/dd/yy>*	*<name>*	*<mm/dd/yy>*	*<description of change>*

TABLE OF CONTENTS

INTRODUCTION

1.1 PURPOSE OF THE SECURITY APPROACH

Defining a security approach for a project provides a line of site from business requirements through team members and components all the way to implemented security controls. It documents clear responsibilities for implementation, certification, and accreditation of the system security and provides a framework for communicating security based impacts on other development and project management activities. This security approach defines from a security perspective how systems associated with the *<Project Name>* project will be characterized, categorized, and managed.

2 SECURITY APPROACH

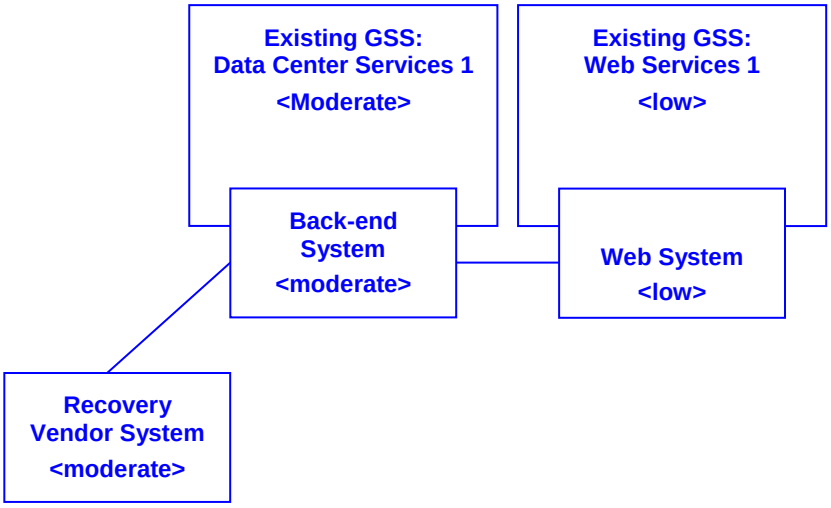
2.1 PROCESS OVERVIEW

[Summarize the steps necessary for establishing the security approach.]
The project manager, working with in collaboration with the security team developed a preliminary assessment of the system's FIPS 199 categorization, and using the proposed project goals defined the following approach to securing the IT system in development. The approach seeks the most cost effective and efficient approach to meeting technical, operational, and managerial security requirements. The approach seeks to ensure that security considerations are effectively integrated with other critical processes such as requirements analysis and risk management throughout the life of the project, and that an early assessment of system classification and boundary definitions are appropriately considered to facilitate development and certification efforts later in the project lifecycle.

2.2 SECURITY APPROACH SUMMARY

[Summarize the overall system approach here. Description should reflect decisions that guided how the system boundaries have been defined and the relative maturity of the systems being developed or modified as well as any system interconnections and dependencies. The relationship with existing systems, internal and external, is critical to defining how to approach the overall security of this system. Identifying a security manager for each system and certifying and accreditation authority early in the process ensures that both development and ongoing maintenance are cost effective and efficient.]

<Provisional High-Level Diagram of Systems with FIPS 199 classification and interconnections identified>



3 TEAM MEMBERS

3.1 CERTIFICATION AND ACCREDITATION TEAM

Project Role	Name
Chief Information Officer	*<name>*
Information System Owner	*<name>*
Senior Information Security Officer	*<name>*
Chief Information Security Officer	*<name>*
Authorizing Official	*<name>*

3.2 SECURITY TEAM

[Define the security stakeholders in this section. Include names, roles and contact information]

Name	Project Role	Security
<name>	System Security Manager	*<system name(s) within scope of responsibility if applicable>*
	Developer	
	Security Critical Partner	
	C&A Authority	

4 SYSTEM CATEGORIZATION

4.1 CORE SYSTEMS

Description – *<System Name>* is a new system under development intended to *[describe system purpose].*
Security Manager – *[Identify the security manager for this system]*
Characterization – *<System Name>* is characterized as a *<GSS, MA, or Other>*.

Categorization – Based on an estimate of FIPS 199 impact, this system is provisionally defined as a *<LOW, MODERATE or HIGH>*
Boundaries – *[Describe at a high-level what security services or components are to be included in the part of the system]*
Dependencies – *[Describe the security services or components being inherited from a GSS or MA]*
Interconnections – *[Describe other system interconnections established for data sharing, business continuity, or backup]*

4.2 SUB-SYSTEMS

Description – *<System Name>* is a new system under development intended to <describe system purpose>.
Security Manager – *[Identify the security manager for this system]*
Characterization – *<System Name>* is characterized as a *<GSS, MA, or Other>*.
Categorization – Based on an estimate of FIPS 199 impact, this system is provisionally defined as a *<LOW, MODERATE or HIGH>*
Boundaries – *[Describe at a high-level what security services or components are to be included in the part of the system]*
Dependencies – *[Describe the security services or components being inherited from a GSS or MA]*
Interconnections – *[Describe other system interconnections established for data sharing, business continuity, or backup]*

4.3 INTERCONNECTED SYSTEMS

Description – *<System Name>* is a new system under development intended to <describe system purpose>.
Security Contact – *[Include contact information for this system]*
Interconnections – *[Describe other system interconnections established for data sharing, business continuity, or backup]*

5 PROGRAMMATIC ACTIVITIES

[Use this section to define administrative and management activities that support the overall security approach. These include activities such as training, configuration management, risk management, and communication plans.]

5.1 TEAM TRAINING

[Outline specific training related to security. Include any database or developer training that applies to development activities. Include any specific rules of behavior or special security considerations on which team members need to be educated.]

5.2 REQUIREMENTS MANAGEMENT

Baseline security requirements for each system have been integrated into the Requirements Management process documented in *<Project Management or*

Requirements Management document name> located on *<full network path location>*.

5.3 CONFIGURATION MANAGEMENT

Baseline security requirements for each system have been integrated into the Configuration Management process documented in *<Project Management or Configuration Management document name>* located on *<full network path location>*.

5.4 RISK MANAGEMENT

Baseline security requirements for each system have been integrated into the Risk Management process documented in *<Project Management or Risk Management document name>* located on *<full network path location>*.

5.5 CHANGE MANAGEMENT

Baseline security requirements for each system have been integrated into the Change Management process documented in *<Project Management or Change Management document name>* located on *<full network path location>*.

Appendix A: Security Approach Approval

The undersigned acknowledge that they have reviewed the ***<Project Name>*** **Security Approach** and agree with the information presented within this document. Changes to this **Security Approach** will be coordinated with, and approved by, the undersigned, or their designated representatives.

[List the individuals whose signatures are desired. Examples of such individuals are Business Owner, Project Manager (if identified), Designated Approving Authorities and any appropriate stakeholders. Add additional lines for signature as necessary.]

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

APPENDIX B: REFERENCES

[Insert the name, version number, description, and physical location of any documents referenced in this document. Add rows to the table as necessary.]

The following table summarizes the documents referenced in this document.

Document Name	Description	Location
<Document Name and Version Number>	*<Document description>*	*<URL or Network path where document is located>*

APPENDIX C: KEY TERMS

The following table provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

Term	Definition
[Insert Term]	*<Provide definition of term and acronyms used in this document.>*

APPENDIX D: RELATED DOCUMENTS

- **FIPS 199**, *Standards for Security Categorization of Federal Information and Information Systems*
- **FIPS 200**, *Minimum Security Requirements for Federal Information and Information Systems*
- **SP 800-18**, *Guide for Developing Security Plans for Federal Information Systems*
- **SP 800-30**, *Risk Management Guide for Information Technology Systems*
- **SP 800-37**, *Guide for the Security Certification and Accreditation of Federal Information Systems*
- **SP 800-53**, *Recommended Security Controls for Federal Information Systems*
- **Draft SP 800-53A**, *Guide for Assessing the Security Controls in Federal Information Systems*
- **SP 800-55**, *Security Metrics Guide for Information Technology Systems*
- **SP 800-60**, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- **SP 800-70**, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*
- **SP 800-100**, *Information Security Handbook: A Guide for Managers*