CMS Information Security Policy/Standard Risk Acceptance

Component:	**System Name:**	**Subsystem:**	**Date:**
CMS System Security Level (FIPS-199 Categorization of information system): **High** ☐ **Moderate** ☐ **Low** ☐		**Requestor:**	**Phone Number:**

Overview of the Risk Acceptance Request (explain what is being requested)**:**

Applicable Policy/Standard Affected (include brief description)**:**

Finding from Audit: Not Applicable ☐

1) Finding title and finding #:
2) Risk level: High ☐ Moderate ☐ Low ☐
3) Source of finding:
4) Copy finding text in quotes:
5) Recommendation (copy recommendation text from source text in quotes):
6) Business Risk (describe the exposure to CMS business):

Business Justification for the Risk Acceptance (What is the business impact to CMS of not accepting the request**):**

Justification for Request (Explain why compliance with this policy/standard is not possible due to technical limitations, conflict with mission requirements, or other circumstances)**:**

Risk Mitigation:

1) Describe the compensating controls that will be implemented and, if applicable, the control number from NIST SP 800-53 to reduce the risk of otherwise complying with the policy/standard:

2) Describe how the compensating controls in step 1 provide an equivalent security capability or level of protection for the information system:

Additional Comments: Describe any additional information that may be needed or reference any attachments:

Endorsement of Risk Analysis Understanding and Acceptance

Concur ☐ **Non-Concur** ☐ **See Comments** ☐ _____ _____

Business Owner & Title Date

Comments:_____

_____

_____

Concur ☐ **Non-Concur** ☐ **See Comments** ☐ _____ _____

Information System Security Officer Date

Comments:_____

_____

_____

Concur ☐ **Non-Concur** ☐ **See Comments** ☐ _____ _____

Authorizing Official & Title Date

Comments:_____

_____

_____

_____

Please note: If granted, this risk acceptance must be reviewed at least annually by the requesting component. Waivers must be renewed every three years or when significant changes which affect the system categorization, justification for noncompliance and/or compensating controls are made.