<Memo Date>

MEMORANDUM TO: <System Owner First Name MI Last Name>, <Title>

FROM: <Authorizing Official First Name MI, Last Name>, Director/Secretary

SUBJECT: AUTHORITY TO OPERATE <SYSTEM NAME>

After reviewing the enclosed system security documentation, it has been determined that the risk to agency operation, assets, and individuals resulting from the operation of this information system is acceptable. This memorandum authorizes the operation of <System Name>. The supporting accreditation was developed and reviewed to ensure that the system complies with OITS and State of Kansas Standards.

<System Name or Acronym> is categorized as a <System Security Categorization level> <System Name or Acronym> and must be reauthorized to operate within three years of the date of this memo or when a significant change occurs. The authorization termination date can be adjusted by the Authorizing Official to reflect an increased level of concern regarding the security state of the information system.)

The information system is authorized to operate for a specified time period of three years in accordance with the terms and conditions established and listed in the enclosure by the authorizing official.

Attachments:

Security Document Review

Terms and Conditions

Signature Page

cc:

(CISO), CISO

(CITO), CITO

The following table identifies the system security documentation that was reviewed.

|  |  |
| --- | --- |
| **Document Title** | **Review Date** |
| System Security Plan |  |
| Continuous Monitoring Plan |  |
| Risk Assessment |  |
| Security Assessment |  |
| Disaster Recovery Plan and Testing Results |  |
| Business Impact Analysis |  |
| Plan of Action and Milestones (POA&M) |  |

The information system is authorized to operate without any significant restrictions or limitations. This security authorization is our formal declaration that adequate security controls have been implemented in the information system in its existing location and that a satisfactory level of security is present. This security authorization will remain in effect as long as the System Owner satisfies OITS and State of Kansas policies and security requirements, the periodic assessments of security controls do not reflect an increase in an unacceptable level of risk, and the general and system-specific conditions provided below are met.

General Conditions

1. Continuous monitoring and scanning must be performed in accordance with OITS and State of Kansas Policies
2. All weakness and deficiencies identified by security assessments, risk assessments, vulnerability assessments, and audits are included in the system POA&M, tracked, and statuses updated regularly.
3. The Chief Information Technology Officer and the Chief Information Security Officer must be informed of any risks that impact the system security posture
4. The system owner must obtain a system reauthorization letter upon any significant change to the system or every three years

This attestation and authorization are accepted by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorizing Official (Signature) Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorizing Official (Print Name)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

System/Application Owner (Signature) Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

System/Application Owner (Print Name)