USAi-{{Agency}}

Customer Responsibility Matrix (CRM)

System Security and Privacy Plan (SSPP)

[Date]

## Document Prepared By

| Organization Name | {{Agency}} |
| --- | --- |
| Address Line 1 |  |
| Address Line 2 |  |
| City, State Zip |  |

## Document Revision History

| **Date** | **Comments** | **Version** | **Author** |
| --- | --- | --- | --- |
| 9/22/2025 | USAi Initial CRM SSPP | V1.0 | USAi Team (Ryan Palmer) |
|  |  |  |  |
|  |  |  |  |

## Approvals

***Instructions****: If PII is not in scope, delete the Privacy Analyst signature block.*

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

[Name]

System Owner

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

[Name]

Information System Security Officer

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

[Name]

Vendor Information System Security Officer

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

[Name]

Information System Security Manager

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

[Name]

Privacy Analyst

## 

## 1. Solution Name

This SSPP provides an overview of {{solution\_name}} ({{solution\_acronym}}) as implemented by {{agency}}, and explains how customer responsibilities are met to protect data transmitted, processed, or stored by the solution.

***Instruction:*** *Summarize mission/business need and how {{agency}} uses {{service\_name}} (e.g., AI assistant for drafting, search, summarization, code assistance.*

**Table 1-1. Solution Name**

| Cloud Solution Name: | {{solution\_name}} |
| --- | --- |
| Cloud Solution Acronym/Abbreviation: | {{solution\_acronym}} |

## 2. Solution Categorization

The overall FIPS 199 information system security categorization is **{{Impact Level}}**

***Instructions:*** *A FIPS 199 Security Categorization document must be completed and submitted as an Attachment to this SSPP.*

### 2.1 Information Types

The following table identifies the information types and impact levels that are input, stored, processed, and/or output from the {{solution\_name}} environment. The security impact levels for confidentiality, integrity, and availability for each of the information types are expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS 199 (Note: The information types found in NIST SP 800-60, Volumes I and II, Revision 1 are the same information types found in the Federal Enterprise Architecture (FEA) Consolidated Reference Model).

### Table 2-1. Information Types

***Instructions:*** *The following information types are provided as illustrative examples of data that agencies may commonly encounter when deploying AI chatbot or API solutions in support of normal operations. These examples are drawn from the NIST SP 800-60 Volume II taxonomy. Please complete the FIPS-199 worksheet in Appendix A.*

*Agencies must conduct their own analysis to review, tailor, and update the applicable information types according to their specific business processes, system functions, and data usage. Final determinations of confidentiality, integrity, and availability (CIA) impact levels should be made by each agency as part of its risk management framework (RMF) activities.*

| **Information Type** | **Confidentiality** | **Integrity** | **Availability** |
| --- | --- | --- | --- |
| *C.2.6.1 – Customer services* | *Low* | *Low* | *Low* |
| *C.2.6.2 – Official information dissemination* | *Low* | *Low* | *Low* |
| *C.2.8.9 – Personal identity and authentication information* | *Moderate* | *Moderate* | *Moderate* |
| *C.2.8.12 – General information* | *Low* | *Low* | *Low* |
| *C.3.1.2 – Help desk services* | *Low* | *Low* | *Low* |
| *C.3.4.4 – Services acquisition* | *Low* | *Low* | *Low* |
| *C.3.5.1 – System development* | *Low* | *Moderate* | *Low* |
| *D.20.2 – General purpose data and statistics* | *Low* | *Low* | *Low* |
| *D.21.1 – Inspections and auditing* | *Moderate* | *Moderate* | *Low* |
| *C.2.6.1 – Customer services* | *Low* | *Low* | *Low* |
| *C.2.3.4 – Strategic planning* | *Low* | *Low* | *Low* |

### 2.2 Potential Impacts of Security Objectives

Based on the information provided above, the potential impacts for each security objective, per Appendix A FIPS 199) for the {{solution\_name}} environment is summarized in the table below.

**Table 2-2. Security Objective Impacts**

| **Security Objective** | **Impact Level** |
| --- | --- |
| Confidentiality | Moderate |
| Integrity | Moderate |
| Availability | Moderate |

### 2.3 Digital Identity Acceptance Statement

*Instructions: Summarize assurance levels per NIST SP 800‑63 see (Appendix B: Digital Identity Worksheet)*

**Table 2-3. Digital Identity Acceptance Statement Assurance Level Summary**

| **Assurance Levels** | **Implemented Assurance Level** |
| --- | --- |
| **Identity Assurance Level (IAL)** | Choose a level |
| **Authentication Assurance Level (AAL)** | Choose a level |
| **Federation Assurance Level (FAL)** | Choose a level |

## 3. Information System Owner

The following individual is identified as the System Owner for this {{solution\_name}}.

| Name |  |
| --- | --- |
| Title |  |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

## 4. Authorizing Official

The Authorizing Official (AO) for this {{solution\_name}} is identified below.

| Name |  |
| --- | --- |
| Title |  |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

## 5. Assignment of Security Responsibility

The Information System Security Manager (ISSM) has been appointed and is identified below.

| Name |  |
| --- | --- |
| Title |  |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

The Information System Security Officer (ISSO) has been appointed and is identified below.

| Name |  |
| --- | --- |
| Title |  |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

## 6. Other Designated Contacts

The individual(s) identified below possess in-depth knowledge of this {{solution\_name}} and/or its functions and operation.

| Name |  |
| --- | --- |
| Title | Agency AI Lead/CAIO |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

| Name |  |
| --- | --- |
| Title | Agency Integration POC |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

## 7. {{solution\_name}} Operational Status

The {solution\_name}} is currently in the life-cycle phase noted in the following table.

**Table 7-1. System Operational Status**

| **System Operational Status** | **Status Description** |
| --- | --- |
| ☐ Operational | The system is operating and in production. |
| ☐ Under Development | The system is being designed, developed, or implemented. |
| ☐ Major Modification | The system is undergoing a major change, development, or transition. |
| ☐ Other | Explain: |

## 8. General System Description

USAi is a centralized generative AI service from GSA that provides federal agencies with access to a selection of vetted artificial intelligence models. The service is designed to streamline procurement, accelerate AI adoption, and ensure consistent security for common government use cases.

Core capabilities include chat, API access, code completion supported by features such as document upload and web search. Security is managed centrally to reduce the compliance burden on individual agencies, with the service operating within a secure environment. The USAi service is NOT FedRAMP authorized, but operates on FedRAMP authorized cloud and uses AI models spruced from FedRAMP authorized cloud services.

***Instruction:*** *Reference provider documentation for general description; describe {{agency}}‑specific mission use, data types, and guardrails.*

{{agency}} uses USAi to:

| **Use Case** | **Purpose / Agency Use Case** |
| --- | --- |
| *Example:*  *General Chat* | *General staff productivity, drafting public communications.* |

# 

## 9. System Environment and Authorization Boundary

This section describes the operational environment for {{agency}}'s use of the USAi service and defines the authorization boundary. The authorization boundary includes all the components that are owned, operated, and managed by {{agency}} as part of its consumption of the USAi service. Components managed by the USAi service provider (GSA) are considered external to this boundary but are essential interconnected systems.

***Instruction:*** *The purpose of this section is to define the logical boundary for the agency's configuration and data within the USAi service. The narrative should focus only on the elements the agency directly controls inside the USAi tenant, treating the underlying agency network and the USAi platform as separate, interconnected entities.*

### 9.1 Boundary Narrative

The authorization boundary for {{agency}}'s implementation of USAi begins at the agency's user endpoints and extends through the agency's network infrastructure to the connection point with the USAi service.

Components and Data Within the {{agency}} USAi Authorization Boundary:

* **Tenant Configuration:** All agency-specific settings managed via the USAi Console and Chat, including enabled AI models, system-level prompts.
* **Access Control Configuration:** The assignment roles and permissions defined within the USAi tenant.
* **Service Credentials:** API keys and other service account credentials generated by {{agency}} api managers or users within the USAi tenant for programmatic access.
* **Agency Data:** All prompts, uploaded documents, and output generated by {{agency}} users and stored within the USAi tenant. The agency is the data owner and is responsible for its content in accordance with the policies outlined in this plan.
* **Log Data:** The audit and interaction logs generated by the USAi tenant made available to the Agency for ingestion into external systems.

Components that interact the {{agency}} USAi Authorization Boundary include:

* **Agency General Support System (GSS):** Includes agency-managed end-user devices (GFE), the enterprise network (firewalls, proxies), and other common controls.
* **Agency Identity Provider (IdP):** The {{idp\_name}} service that provides authentication for agency users.
* **Agency Security Operations Center (SOC) Infrastructure:** The {{siem\_name}} and other tools that receive and analyze logs from USAi.

**External Provider Systems Outside the Boundary:**

The core USAi platform, managed by GSA, is external to this boundary. This includes the application itself, the underlying cloud infrastructure, and the interconnected AI models.

### 9.2 Information System Web Site URL Addresses

The following table lists the web site URL addresses for {{solution\_name}}.

### Table 9-1 System URLs

| **System Component** | **Application URL** | **Public or Private** |
| --- | --- | --- |
| chat | chat.{{agency}}.usai.gov | Private |
| api | api.{{agency}}.usai.gov | Private |
| Console | console.{{agency}}.usai.gov | Private |

### 9.3 Types of Users

***Instruction****: For an External User, please enter N/A” in the Sensitivity Level column. Please include systems administrators and database administrators as role types. (Include solution administrators, managers, etc.). Add additional rows if necessary.*

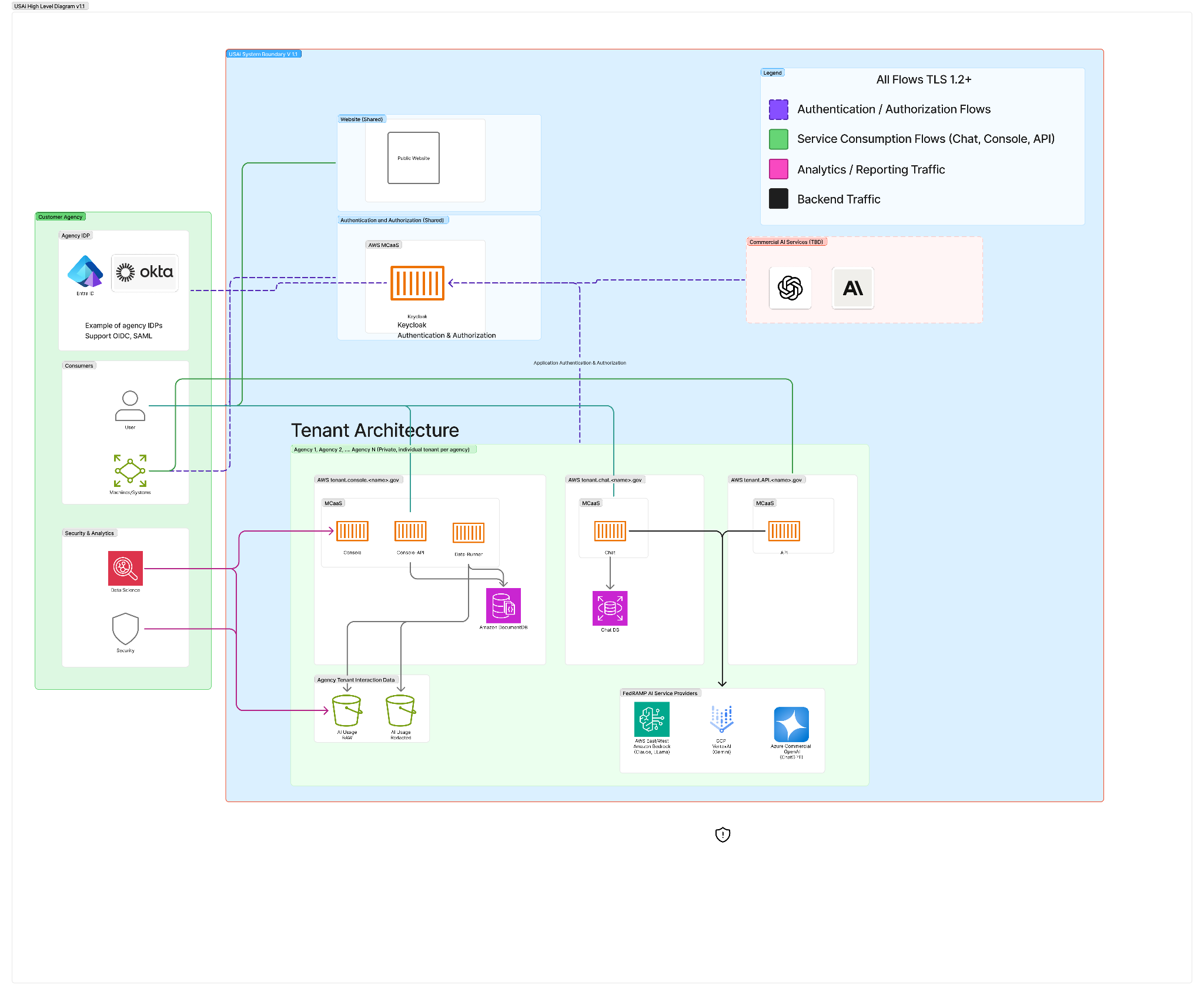
All users have their employee status categorized with a sensitivity level in accordance with PS-2. Employees (or contractors) of {{agency}} are considered Internal Users. All other users are considered External Users.

### Table 9-2 User Roles and Privileges

| **Role** | **Internal or External** | **Privileged (P), Non-Privileged (NP)** | **Sensitivity Level** | **Authorized Privileges** | **Functions Performed** | **MFA Authentication Method** |
| --- | --- | --- | --- | --- | --- | --- |
| **USAi-tenant administrator** | Internal | **Privileged** | Medium | Full administrative control within the agency scope | Manage models, chat configuration, api keys | *{{Agency-IDP}}* |
| **API-key-managers** | Internal | **Privileged** | Medium | Issue short-lived API keys (≤1 day); revoke issued keys | Provision and revoke developer API keys for project work | *{{Agency-IDP}}* |
| **Default-user** | Internal | **Non-Privileged** | Low | Baseline safe defaults | Console sign-in; chat with agency-approved models only. No key issuance, or settings changes | *{{Agency-IDP}}* |
| **api-user** | Internal | **Non-Privileged** | Low/Medium | API key used to connect with the solution | Enable applications/systems to call APIs with an issued key with approved models | N/A (key-based auth) |

### 9.4 Illustrated Architecture and Narratives

A high-level diagram from the USAi SSPP is provided below for reference.



***Instruction****: Separately identify your {{agency}} specific integrations with the USAi service. For example, if your agency uses Okta for authentication, describe that integration.*

USAi is a government shared service that resides in the AWS East/West and leverages AI services from Azure Commercial, Google GCP and AWS East/West.

{{agency}} integrates with the following services: [Describe the integrations here, e.g., "GSA integrates with Okta for identity management and ServiceNow for ticketing."]

### Table 9-3 Standard Integrations

| **Category** | **Technical Solution** |
| --- | --- |
| IAM/Access Management | {{Agency-IDP}}: User Authentication and SSO |
| Ticketing | {{Agency-Ticketing System}}: Change and issue tracking |
| Firewall/VPN | Solutions/IPP address use to access the system |
| SIEM | {{Agency-SIEM}} |

### 

***Instruction****: Separately identify any additional integrations with the agency system with USAi and the means of integration.*

### Table 9-4 Additional Integrations & Access Requirements

| **Category** | **System** | **Services (chat,api,console)** | **Source IP Space** |
| --- | --- | --- | --- |
| Integration 1 |  |  |  |
| Integration 2 |  |  |  |
| Integration 3 |  |  |  |
| Integration 4 |  |  |  |

### 9.5 Commercial AI chatbot integration

***Instruction****: Use this section to document any commercial, direct-to-web AI chatbot services (e.g., 'OneGov AI' or 'Quick Buy' deals) that your agency wishes to access through the USAi portal. For each service, complete the table below. Note that your agency is solely responsible for the risk assessment, security compliance, and authorization of these external services*

**Guidance: Before integrating, your agency should follow a process similar to the "Quick Buy" steps:**

* Conduct a thorough risk assessment and review of the provider's security practices.
* Review the GSA AI Standard Terms and Conditions.
* Issue a separate Authority to Operate (ATO) or other risk acceptance documentation based on your agency's policies.
* Establish clear internal guidelines on what data types (e.g., PII, CUI) are permitted for use with the service.

In addition to its core capabilities, the USAi platform can be configured to act as an authentication gateway or central access portal to separately procured commercial AI services. It is critical to understand that these commercial services **operate outside the USAi authorization boundary.**

USAi's role in this context is limited to brokering user access, typically by providing a federated sign-on (SSO) capability or a direct link from the USAi portal. The customer agency remains fully responsible for the governance, security, and compliance of its use of these external services. The table below serves as the official inventory of these integrated commercial services and documents the agency's due diligence.

### Table 9-5 Integrated Commercial AI Services

| **Commercial Service Name & Provider** | **Purpose / Agency Use Case** | **Data Sensitivity Allowed (Per Agency Policy)** | **Agency Authorization Status (e.g., Full ATO, Pilot ATO, Risk Acceptance)** | **USAi Integration Method (e.g., Portal Link, SAML Federation)** |
| --- | --- | --- | --- | --- |
| *Example:*  *ChatGPT Enterprise (OpenAI)* | *General staff productivity, drafting public communications.* | *Public data only. No PII or CUI.* | *Temporary ATO issued [Date]* | *Federated with USAi Authentication and Agency Auth* |
| *Example:*  [*Calude.ai*](http://calude.ai)  *(anthropic)* | *General staff productivity, drafting public communications.* | *Public data only. No PII or CUI.* | *Temporary ATO issued [Date]* | *Federated with USAi Authentication and Agency Auth* |

# 

# **10. USAi CRM Requirements**

The full implementation of all controls required for USAi are inclusive of both GSA vendor controls and customer responsibilities as outlined in the USAi Customer Responsibility Matrix. Please refer to the GSA USAi SSPP for vendor responsible control implementation statements. The following sections describe {{agency}}'s implementation of customer responsibilities as identified in the CRM.

### 

| **CR #** | **Domain** | **Short Title** | **Controls Reference** |
| --- | --- | --- | --- |
| CR‑1 | Identity & Access | Federate IdP with {{service\_name}} | AC‑2(1)/3/6/17, IA‑2/4/5/8 |
| CR‑2 | Identity & Access | Enforce phishing‑resistant MFA | IA‑2/5, OMB M‑22‑09 |
| CR‑3 | Identity & Access | Least‑privilege role assignments | AC‑2/AC‑6 |
| CR‑4 | Identity & Access | Rotate/disable dormant service creds | AC‑2(3), IA‑5 |
| CR‑5 | Identity & Access | Periodic access reviews | AC‑2(7), AU‑6 |
| CR‑6 | Encryption | Enforce TLS 1.2+ to UI/API | SC‑8/8(1), SC‑13 |
| CR‑7 | Data Handling | Enforce input restrictions / redaction | PL-4, RA-3, SI-12 |
| CR‑8 | Data Handling | User policy & training for public instances | AT‑2, PL‑4 |
| CR‑9 | Network/Session | Secure agency endpoints & networks | SC‑7, SC‑23 |
| CR‑10 | Logging | Ingest {{service\_name}} security logs | AU‑2/3/6/9 |
| CR‑11 | Logging | Ingest logs from integrated offerings | AU‑2/3/6/9 |
| CR‑12 | Logging | Weekly privileged‑action review | AU‑6 |
| CR‑13 | Vulnerability | Manage vulns on agency systems | RA‑5, SI‑2 |
| CR‑14 | Vulnerability | Participate in disclosure/bug bounty | RA-5(11) |
| CR‑15 | Change Mgmt | Manage/document tenant settings | CM‑2/3/6/7 |
| CR‑16 | Change Mgmt | Approve security‑impacting changes | CM‑3/4 |
| CR‑17 | Governance | Inventory privileged users/keys | CM‑8, PM‑5 |
| CR‑18 | Governance | Document use, risk, and authorization | PL‑2, CA‑6/7 |
| CR‑19 | Governance | Develop agency policies/procedures | PL‑2, PM‑5 |
| CR‑20 | Supply Chain | Approve third‑party integrations | SA‑4/12, SR‑3/4/5/6 |
| CR‑21 | Supply Chain | Monitor third‑party integrations | SA‑9, SR‑6 |
| CR‑22 | Models/Services | Review model/service documentation | SA‑4/9, CA‑7 |
| CR‑23 | Recovery | Manage/backup agency data from {{service\_name}} | CP‑2/9 |
| CR‑24 | Recovery | Include {{service\_name}} in BCDR | CP‑2/4/7 |
| CR‑25 | Incident | Notify {{service\_provider}} within SLA | IR‑4/5/6/8 |
| CR‑26 | Incident | Maintain internal incident log; coordinate | IR‑4/6 |
| CR‑27 | Incident | Implement agency IR procedures (AI/chat) | IR‑4/8 |
| CR‑28 | Authorization & Risk | Categorize & authorize usage; privacy | AT‑2, RA‑2, PL‑2/4 |
| CR‑29 | ConMon | Define continuous monitoring plan | CA‑7 |
| CR‑30 | ConMon | Review provider ConMon; track residual risk | CA‑6/7 |
|  |  |  |  |

# 

### CR-1 Federate {{Agency}} IdP with USAi

| **CR-1** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Federate your agency's enterprise Identity Provider (IdP) with the USAi service via SAML 2.0 or OIDC. | |
| **Controls Reference:** AC‑2(1)/3/6/17, IA‑2/4/5/8 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Consult USAi documentation for IdP integration steps. Configure attribute mapping to ensure necessary user information is passed to USAi.*  **Implementation:**  {{agency}} federates {{idp\_name}} with USA using {{idp\_protocol}}. The IdP provides core attributes, email, unique ID, and organizational levels) to enable SSO and role mapping. Direct (non‑federated) sign‑in is disabled. Federation is validated in USAi staging prior to promotion to prod under {{ticketing\_system}} change control with documented rollback. | |
| Artifacts/Evidence (links): IdP app config export, attribute‑mapping doc, screenshots, test plan/results, CAB approval. | |

### CR-2 Enforce phishing‑resistant MFA

| **CR-2** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Enforce phishing-resistant Multi-Factor Authentication (MFA) for all human user access to USAi, in line with federal requirements (e.g., OMB M-22-09, CISA guidance). | |
| **Controls Reference:** IA‑2/5, OMB M‑22‑09 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** Utilize agency-approved phishing-resistant authenticators (e.g., PIV/CAC, FIDO2/WebAuthn security keys) managed through Partner Agency’s federated Identity Provider (IdP).  **Implementation:**  All human access to USAi is protected by phishing‑resistant MFA enforced by {{idp\_name}} at AAL{{aal\_level}}. Allowed authenticators: {{allowed\_authenticators}}. Legacy factors are {{legacy\_factor\_policy}}. MFA applies to UI, admin, and API flows via the IdP. Break‑glass accounts are not used. | |
| Artifacts/Evidence (links): IdP MFA policy, list of allowed authenticators, exception register. | |

### CR-3 Least‑privilege role assignments within USAi

| **CR-3** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Define and assign users to least-privilege roles within USAi | |
| **Controls Reference:** AC‑2/AC‑6 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Map Partner Agency job functions to available USAi roles. Regularly review and adjust role assignments.*  **Implementation statement (starter):**  {{agency}} maps job functions to USAi roles and assigns least privilege by default. Elevated roles require managerial approval and a {{ticketing\_system}} record. Role claims are group‑based in USAi}; temporary elevation is time‑boxed with automatic expiry. Access is re‑certified {{review\_cadence}} and upon personnel changes. | |
| **Artifacts/Evidence (links):** RBAC matrix, approval workflow, group‑to‑role mapping, quarterly recertification attestation. | |

### CR-4 Rotate/disable dormant service creds

| **CR-4** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Disable or rotate credentials for dormant non-human (service) accounts within ≤ 30 days of inactivity (or agency-defined shorter period). | |
| **Controls Reference:** AC‑2(3), IA‑5 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Implement a process to monitor service account activity. Automate credential rotation where possible using secrets management tools.*  **Implementation statement (starter):**  All USAi service accounts are inventoried with named owners. Credentials are stored/rotated by users and automatically and disabled after 1 day for standard user generated API keys or {{long duration api key length}} for those supporting system integration.  Non-user service account logs from USAi are ingested to {{siem\_name}}. Exceptions require {{integration\_approval\_body}} approval and compensating controls. | |
| **Artifacts/Evidence (links):** Service account inventory, rotation policy, SIEM inactivity report, exception log. | |

### CR-5 Periodic access reviews

| **CR-5** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Conduct regular reviews of all user accounts, privileged access, and service accounts. | |
| **Controls Reference:** AC-2, AC‑2(7)\* | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Establish a quarterly (or more frequent, based on risk) review cycle. Document reviews and any actions taken (e.g., de-provisioning, role changes).*  **Implementation statement (starter):**  On a {{review\_cadence}} cadence, {{agency}} exports {{service\_name}} users and non-person entities, reconciles against HR/contractor rosters, and removes or downgrades access via {{ticketing\_system}}. Privileged accounts are additionally spot‑checked {{privileged\_log\_review\_cadence}} for appropriateness. | |
| **Artifacts/Evidence (links):** Recertification report, rosters, de‑provision tickets, sampling checklist. | |

### CR-6 Enforce TLS 1.2+ to USAi

| **CR-6** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Ensure all agency network traffic to USAi chat UI and API endpoints utilizes TLS 1.2 or higher. | |
| **Controls Reference:** SC‑8/8(1), SC‑13 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Configure Partner Agency network devices (proxies, firewalls, VPN) and client applications to enforce TLS 1.2+ for connections to USAi services.*  **Implementation statement (starter):**  All traffic to {{service\_name}} UI/API is forced through {{proxy\_firewall}} with TLS 1.2+ (TLS 1.3 preferred). Deprecated ciphers/protocols are blocked. Egress allow‑lists limit destinations to {{service\_name}} endpoints. Configuration is reviewed {{review\_cadence}} and on provider endpoint changes. | |
| **Artifacts/Evidence (links):** Firewall/proxy/VPN policy export, cipher policy, egress allow‑list, change tickets. | |

### CR-7 Enforce input restrictions / redaction

| **CR-7** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Manage and enforce internal policies regarding user input of sensitive data (e.g., PII, CUI). If agency policy prohibits submitting such data to USAi, the agency is responsible for ensuring users tokenize, redact, or de-identify data before submission, in alignment with its risk posture and data sensitivity guidelines. | |
| **Controls Reference:** PL-4, AT-2, PL-2, SC-28(1), if PII is in scope, PT-2, PT-3 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:***  *Develop internal agency guidance and training on appropriate data handling for AI services. Leverage USAi-provided tools (if any) or approved third-party solutions for data masking or redaction. Review USAi service security information and vendor-specific documentation for data handling best practices.*  **Implementation statement (starter):**  {{agency}} policy defines permitted/prohibited data for USAi (e.g., {{data\_categories}}). Users must tokenize/redact prohibited data using {{dlp\_or\_redaction\_tool}} prior to submission. The USAi training and login page includes reminders, periodic sampling and coaching are conducted. Violations are addressed via the {{process}} | |
| **Artifacts/Evidence (links):** Policy link, user training deck, tool configuration, sampling results, IR playbook. | |

### CR-8 User policy & training for public instances

| **CR-8** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  For public-facing or broadly accessible USAi instances, establish clear usage policies and training for end-users regarding appropriate data input. | |
| **Controls Reference:** AT‑2, PL‑4 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Develop and disseminate user agreements and training materials that explicitly state what types of information are permissible and prohibited for input into these instances.*  **Implementation statement (starter):**  For public/broad USAi usage instances, {{agency}} publishes an AI Acceptable Use Policy, requires acknowledgement at onboarding, and provides annual refresher training. UI banners remind users about prohibited inputs. Non‑compliance results in access revocation. | |
| **Artifacts/Evidence (links):** AUP link, LMS records, UI screenshot, enforcement SOP. | |

### CR-9 Secure agency endpoints & networks

| **CR-9** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  This capability is primarily managed by the USAi Service. Secure Partner Agency endpoints and networks connecting to USAi. | |
| **Controls Reference:** SC-7, SC-23 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Ensure agency endpoints meet baseline security configurations and that network controls (firewalls, IDS/IPS) are in place to protect agency assets.*  **Implementation statement (starter):**  Endpoints accessing USAi comply with {{agency}} baseline hardening and run {{edr\_tool}} with real‑time protection. Network controls ({{proxy\_firewall}}, IDS/IPS, VPN) enforce domain allow‑listing and session protections. Remote access follows {{agency}} remote access policy aligned to session management requirements. | |
| **Artifacts/Evidence (links):** Baseline config, EDR policy, allow‑list, IDS/IPS signatures, remote access policy. | |

### CR-10 Ingest USAi security logs

| **CR-10** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Ingest security logs (e.g., authentication, authorization, administrative, and interaction logs actions – retain per agency policy) | |
| **Controls Reference:** AU‑2/3/6/9 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Configure integration between the agency SIEM/SOC and the USAi tenant's designated log export mechanism (e.g., S3 bucket, API). Ensure log formats are compatible and parsing rules are established.*  **Implementation statement (starter):**  USAi authentication, authorization, admin, and interaction logs are exported via {{log\_export\_method}} and ingested to {{siem\_name}}. Parsers preserve timestamps, user IDs, session IDs, and actions. Alerts cover anomalous access, failed login spikes, and sensitive config changes. Logs are retained per {{agency}} policy. | |
| **Artifacts/Evidence (links):** Log pipeline diagram, parser configs, sample events, alert rules, retention settings. | |

### CR-11 Ingest logs from integrated commercial offerings (e.g. [chatgpt.com](http://chatgpt.com), claude.ai)

| **CR-11** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Ingest available logs from integrated commercial offerings as per Partner Agency requirements and the capabilities of the offering. | |
| **Controls Reference:** AU‑2/3/6/9 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Review documentation for each commercial offering to determine available log types and integration methods.*  **Implementation statement (starter):**  For each enabled integration (e.g., {{example\_integrations}}), {{agency}} enables available audit logs and forwards them to {{siem\_name}}. Where audit logs are unavailable, a risk is logged in {{poam\_repository}} with compensating detective controls. | |
| **Artifacts/Evidence (links):** Integration inventory, vendor log capability matrix, SIEM data source list, POA&M entries. | |

### CR-12 Privileged‑action review

| **CR-12** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Review privileged-action logs within USAi at least weekly (or more frequently based on risk). | |
| **Controls Reference:** AU-6 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Establish a documented process for this review, assign responsibility, and define criteria for escalating suspicious activity. Consider automated alerting for high-risk privileged actions.*  **Implementation statement (starter):**  At least {{privileged\_log\_review\_cadence}}, {{agency}} reviews privileged actions (role changes, API key creation, export/retention changes) in USAi. High‑risk events generate real‑time alerts. Findings and dispositions are tracked in {{ticketing\_system}}; confirmed issues follow IR procedures. | |
| **Artifacts/Evidence (links):** Review checklist, alert definitions, tickets, meeting notes. | |

### CR-13 Manage vulns on agency systems

| **CR-13** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Agencies are responsible for managing all vulnerabilities on Partner Agency systems that connect to USAi. | |
| **Controls Reference:** RA‑5, SI‑2 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Partner Agency must follow its internal vulnerability management program for its own assets and use of USAi.*  **Implementation statement (starter):**  Systems that access or integrate with {{service\_name}} are scanned by {{vuln\_scanner}} on a {{review\_cadence}} cadence. Remediation follows {{agency}} SLAs (e.g., Critical 15, High 30d). Patching is orchestrated via {{patching\_tool}} with follow‑up scans to verify closure. | |
| **Artifacts/Evidence (links):** Scan results, remediation tickets, SLA dashboard, exception register. | |

### CR-14 Participate in disclosure/bug bounty

| **CR-14** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Participate in the USAi vulnerability disclosure and/or bug bounty program, if available and applicable. | |
| **Controls Reference:** RA-5 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Designate point(s) of contact within Partner Agency to receive security notifications from GSA. Follow GSA-provided procedures for reporting potential vulnerabilities discovered by the Partner Agency.*  **Implementation statement (starter):**  {{agency}} designates security POCs to receive {{service\_provider}} advisories and report suspected USAi vulnerabilities via gsa-ir@gsa.gov. Internal findings are triaged in {{ticketing\_system}} and relayed to gsa-ir@gsa.gov with minimal necessary detail per safe‑harbor/VDP terms. | |
| **Artifacts/Evidence (links):** POC list, VDP procedure, sample submission, ticket linkage. | |

### CR-15 Manage/document tenant settings

| **CR-15** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Manage and document all Partner Agency-configurable tenant settings within USAi (e.g., user settings, role mappings, integration configurations) in accordance with Partner Agency change management policies. | |
| **Controls Reference:** CM‑2/3/6/7 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Utilize the USAi administrative console for configurations. Maintain a record of changes, approvals, and testing. Periodically audit configurations against agency baselines.*  **Implementation statement (starter):**  {{agency}} baselines all USAi tenant settings (authn/z, roles, integrations, data retention, logging). Changes require {{ticketing\_system}} records, peer review, and testing before general availability. Periodic audits compare running config to the approved baseline; deviations go to {{poam\_repository}}. | |
| **Artifacts/Evidence (links):** Baseline config, change records, audit reports, POA&M entries. | |

### CR-16 Approve security‑impacting changes

| **CR-16** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Review and approve any significant configuration changes related to security or data access within the USAi tenant. | |
| **Controls Reference:** CM‑3/4 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:***   * *Integrate USAi into a Partner Agency's System Security Plan (SSP) or maintain a dedicated SSP for the agency's use of USAi (THIS).* * *Ensure risk assessments are performed and documented based on agencies' usage of USAi.*   **Implementation statement (starter):**  Changes affecting security or data access (IdP integration, role models, data sharing, log routing) require {{integration\_approval\_body}} approval with risk/privacy assessment and rollback plans. Approvals are recorded in {{ticketing\_system}}; communications to stakeholders occur before production change. | |
| **Artifacts/Evidence (links):** Risk assessment template, CAB/ARB minutes, approval ticket, rollback plan. | |

### CR-17 Inventory privileged users/keys

| **CR-17** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Maintain an up-to-date inventory of all privileged users, service accounts, API keys, and critical integration points associated with the agency's USAi tenant. | |
| **Controls Reference:** CM‑8, PM‑5 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Conduct regular (e.g., quarterly) reviews and reconciliations of this inventory. Store API keys and sensitive credentials securely, following agency best practices for secrets management.*  **Implementation statement (starter):**  {{agency}} maintains an inventory of USAi privileged users, service accounts, API keys/secrets, and critical integrations with owners, purpose, and expiry. Keys/secrets are stored in {{secrets\_manager}} with rotation policies. The inventory is reconciled {{review\_cadence}} and on personnel changes. | |
| **Artifacts/Evidence (links):** Inventory register (system report), rotation policy, reconciliation report. | |

### CR-18 Document use, risk, and authorization

| **CR-18** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Document how the USAi service (and any integrated commercial offerings) are used to meet Partner Agency mission needs, including associated data sensitivity, risk categorizations, and an Authority to Operate (ATO) or approval memo. | |
| **Controls Reference:** PL‑2, CA‑6/7 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Integrate USAi into Partner Agency's System Security Plan (SSP) or maintain a dedicated SSP addendum. Ensure risk assessments are performed and documented.*  **Implementation statement (starter):**  {{agency}} documents USAi mission use cases, data categories, FIPS 199 results, and privacy determinations (PTA/PIA/SORN as applicable). The selected authorization path (e.g., {{authorization\_type}}) and residual risks are recorded in {{poam\_repository}}. The SSPP/addendum is maintained under change control. | |
| **Artifacts/Evidence (links):** SSPP/addendum, FIPS 199, PTA/PIA/SORN, risk register, POA&M. | |

### CR-19 Develop agency policies/procedures

| **CR-19** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Develop and maintain agency-specific policies and procedures for the secure use of USAi services. | |
| **Controls Reference:** PL‑2, PM‑5 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Ensure policies cover acceptable use, data handling, incident reporting, and user responsibilities.*  **Implementation statement (starter):**  {{agency}} maintains policies and SOPs for USAi acceptable use, data handling, IR, and admin operations. Policies are published at {{agency\_policy\_portal\_url}}; compliance is reinforced during onboarding and annually via training. | |
| **Artifacts/Evidence (links):** Policy links, SOPs, training records, attestation logs. | |

### CR-20 Approve third‑party integrations

| **CR-20** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Review and formally approve any agency-initiated plugin, webhook target, custom-developed tool, or third-party application intended for integration with the USAi tenant before enablement. | |
| **Controls Reference:** SA‑4/12, SR‑3/4/5/6 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Conduct a risk assessment for each proposed integration, considering data sensitivity, access permissions, and the security posture of the third-party service/tool. Document approvals.*  **Implementation statement (starter):**  Before enablement, each plugin/webhook/third‑party tool undergoes risk assessment (data types, permission scopes, vendor posture, legal/privacy review) and requires {{integration\_approval\_body}} approval. Integrations are configured for least‑privilege scopes and restricted audiences. | |
| **Artifacts/Evidence (links):** Risk assessment forms, permission scopes, approval record, config screenshot. | |

### CR-21 Monitor third‑party integrations

| **CR-21** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Monitor the security and compliance of approved third-party integrations throughout their lifecycle. | |
| **Controls Reference:** SA‑9, SR‑6 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Periodically re-evaluate the risk of integrated services, especially if their functionality or security posture changes. Be prepared to disable integrations if they no longer meet agency security requirements.*  **Implementation statement (starter):**  Approved integrations are reviewed {{review\_cadence}} or upon material vendor changes. {{agency}} monitors usage, permission drift, and vendor attestations; non‑compliant integrations are disabled and tracked in {{poam\_repository}}. | |
| **Artifacts/Evidence (links):** Review schedule, usage reports, vendor attestations, POA&M entries. | |

### CR-22 Review model/service documentation

| **CR-22** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Review model and service documentation for leveraged services and models. | |
| **Controls Reference:** SA‑4/9, CA‑7 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Periodically re-evaluate the risk of models and services. Perform ongoing performance monitoring of services.*  **Implementation statement (starter):**  {{agency}} maintains an inventory of models/services leveraged by USAi and reviews provider documentation for security, privacy, retention, and update cadence. Significant changes trigger risk reassessment and updates to user guidance and technical guardrails. | |
| **Artifacts/Evidence (links): Model/service inventory, review checklist, change impact assessments.** | |

### CR-23 Manage/backup agency data from USAi

| **CR-23** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Partner Agency must develop procedures for backing up and recovering any critical data they input into or export from USAi, if not otherwise retained by USAi in a manner accessible to the agency for recovery (e.g., exported chat logs, API outputs stored in agency systems). | |
| **Controls Reference:** CP‑2/9 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Partner Agency must develop procedures for backing up and recovering any critical data they input into or export from USAi, if not otherwise retained by USAi in a manner accessible to the agency for recovery (e.g., exported chat logs, API outputs stored in agency systems). Document what data, where data is stored, and at what cadence.*  **Implementation statement (starter):**  {{agency}} identifies data generated or exported from USAi (e.g., chat logs, prompts, outputs, API results) that must be preserved and backs it up to agency‑managed repositories using {{backup\_tool}} with encryption in transit/at rest. Restore procedures are documented and tested {{review\_cadence}}. | |
| **Artifacts/Evidence (links):** Data inventory, backup policy, job configs, restore test records. | |

### CR-24 Include USAi in BCDR

| **CR-24** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Include USAi usage in agency business continuity and disaster recovery (BCDR) plans, particularly for mission-essential functions relying on the service. | |
| **Controls Reference:** CP‑2/4/7 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Identify dependencies on USAi and plan for alternative processes or manual workarounds if the service is unavailable beyond its stated RTO.*  **Implementation statement (starter):**  {{agency}}’s BCDR plan documents USAi dependencies, tolerances (RTO/RPO), and alternate workflows/manual contingencies if {{service\_name}} is unavailable. Periodic exercises validate continuity procedures; lessons learned drive updates. | |
| **Artifacts/Evidence (links):** BCDR plan excerpt, exercise reports, corrective actions. | |

### CR-25 Notify USAi of incidents

| **CR-25** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Report suspected or confirmed security incidents involving the agency's USAi tenant or data to the designated GSA Security Team (or USAi Service Desk) within 1 hour of discovery. | |
| **Controls Reference:** IR‑4/5/6/8 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Follow GSA-provided incident reporting procedures for reporting to GSA. Provide comprehensive details to facilitate investigation.*  **Implementation statement (starter):**  Suspected or confirmed incidents involving USAi or related data are reported to GSA via gsa-ir@gsa.gov within {{incident\_notification\_sla\_hours}} hour(s) of discovery, including scope, indicators, and initial containment. Internal tickets in {{ticketing\_system}} reference the provider case number. | |
| **Artifacts/Evidence (links):** IR SOP, notification template, ticket sample, comms log. | |

### CR-26 Maintain internal incident log; coordinate with USAi

| **CR-26** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Maintain an internal agency incident logs for any USAi-related incidents and cooperate fully with GSA during incident response and investigation activities. | |
| **Controls Reference:** IR‑4/6 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Designate point(s) of contact with Partner Agency for incident response. Update GSA with relevant internal findings until incident closure.*  **Implementation statement (starter):**  {{agency}} records USAi‑related incidents in {{ticketing\_system}} including timeline, affected users/data, actions, and lessons learned. Designated POCs coordinate with GSA until closure; post‑incident reviews address root cause and control improvements. | |
| **Artifacts/Evidence (links):** Incident records, POC list, PIR/RCA docs, action items. | |

### CR-27 Implement agency IR procedures

| **CR-27** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Implement agency-specific incident response procedures for handling incidents related to USAi usage (e.g., data spillage through chat, compromised user accounts). | |
| **Controls Reference:** IR‑4/8 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:*** *Ensure agency IR plans address scenarios specific to AI and chat services, including containment, eradication, and recovery steps relevant to the USAi platform.*  **Implementation statement (starter):**  {{agency}} maintains AI/chat‑specific playbooks (e.g., data spillage, compromised accounts, malicious integration behavior). Playbooks include containment (revoke tokens, disable accounts), eradication, recovery, and notifications (privacy/legal). Exercises are conducted {{review\_cadence}}. | |
| **Artifacts/Evidence (links):** Playbooks, exercise results, updated procedures. | |

### CR-28 Categorize & authorize usage and perform risk analysis

| **CR-28** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Categorize & Authorize Usage. Perform (or update) FIPS 199 categorization and perform data and privacy risk analysis and privacy plans as needed. | |
| **Controls Reference:** AT‑2, RA‑2, PL‑2/4 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:***   * *Identify data types and information types with high sensitivity and allowed use cases* * *Provide employees with policy guidance and training on appropriate data types for the system* * *Conduct a PTA/PIA/SORN as appropriate based on Partner Agency use case(s).*   ***Implementation statement (starter):***  {{agency}} performs FIPS 199 categorization for USAi use cases, identifies sensitive data and allowed use, and completes PTA/PIA/SORN as applicable. Users receive policy and privacy training. Risk decisions/mitigations are documented in {{poam\_repository}} and the {{authorization\_type}} package. | |
| **Artifacts/Evidence (links):** FIPS 199, PTA/PIA/SORN, training records, POA&M entries, authorization memo. | |

### CR-29 Define continuous monitoring plan

| **CR-29** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Define Continuous‑Monitoring (ConMon) Plan. Review continuous monitoring information provided by GSA. | |
| **Controls Reference:** CA‑7 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:***   * *Integrate GSA‑provided monthly ConMon packages (scan results, POA&M updates) into the agency’s workflow.* * *Participate in monthly continuous monitoring calls.*   **Implementation statement (starter):**  {{agency}} defines a ConMon plan for USAi that consumes artifacts (e.g., scans, POA&Ms, change logs) stored at {{conmon\_artifacts\_location}}. Findings are triaged in {{ticketing\_system}}, tracked in {{poam\_repository}}, and reported to stakeholders on a {{review\_cadence}} cadence. | |
| **Artifacts/Evidence (links):** ConMon plan, artifact repository link, triage SOP, dashboards. | |

### CR-30 Review provider ConMon; track residual risk

| **CR-30** | **Responsibility Summary Information** |
| --- | --- |
| Implementation Status:  ☐ Implemented  ☐ Partially Implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable | |
| **Customer Responsibility:**  Review monitoring artifacts, approve or restrict agency use of any non-FedRAMP services, and track residual risk via POA&Ms. | |
| **Controls Reference:** CA‑6/7 | |
| Describe how the customer responsibility is implemented. | |
| ***Guidance:***   * *Review GSA's and vendor security assessments and risk documentation for alignment with agency requirements.* * *Compare GSA assessments to agency requirements; set data-type guardrails for un-authorized services.*   **Implementation statement (starter):**  {{agency}} reviews USAi security assessments and monitoring artifacts against internal requirements, sets guardrails for any services/features outside authorization scope, and records residual risk in {{poam\_repository}}. Material deltas trigger risk reassessment and user/technical control updates. | |
| **Artifacts/Evidence (links):** Assessment reviews, guardrail memo, POA&M entries, communications. | |

# 

# 

# Appendix A: Information Processing Standard (FIPS) 199 Categorization

***Instruction:*** *Review the NIST Special Publication 800-60 Volume 2 Revision 1,“Appendix C: Management and Support Information and Information System Impact Levels,” and “Appendix D: Impact Determination for Mission-Based Information and Information Systems” to assess the recommended impact level for each of the information types. For more information, consult Appendix D.2.*

*After reviewing the NIST guidance on information types, complete Table A.1, Applicable Information Types with security impact levels using NIST SP 800-60 V2 R1. In the first three columns of the table, specify the NIST SP 800-60 V2 R1 recommended impact level. In the next three columns, specify the agency-determined recommended impact level. If the agency-determined recommended impact level does not match the level recommended by NIST, add an explanation in the last column as to why this decision was made.*

Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type. The FIPS 199 is the High watermark for the impact level of all the applicable information types.

Table A.1 uses the NIST SP 800-60 (current revision) Volume II Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories to identify information types with the security impacts.

The following information types are provided as illustrative examples of data that agencies may commonly encounter when deploying AI chatbot or API solutions in support of normal operations. These examples are drawn from the NIST SP 800-60 Volume II taxonomy.

Agencies must conduct their own analysis to review, tailor, and update the applicable information types according to their specific business processes, system functions, and data usage. Final determinations of confidentiality, integrity, and availability (CIA) impact levels should be made by each agency as part of its risk management framework (RMF) activities.

### Table A.1

| **Information Type** | **Recommended Confidentiality Impact Level**  **(NIST SP 800-60 V2 R1)** | **Recommended Integrity Impact Level**  **(NIST SP 800-60 V2 R1)** | **Recommended Availability Impact Level**  **(NIST SP 800-60 V2 R1)** | **{{agency}} Selected Confidentiality Impact Level** | **{{agency}} Selected Integrity Impact Level** | **{{agency}} Selected Availability Impact Level** | **Statement for Impact Adjustment Justification** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| *C.2.6.1 – Customer services* | *Low* | *Low* | *Low* |  |  |  |  |
| *C.2.6.2 – Official information dissemination* | *Low* | *Low* | *Low* |  |  |  |  |
| *C.2.8.9 – Personal identity and authentication information* | *Moderate* | *Moderate* | *Moderate* |  |  |  |  |
| *C.2.8.12 – General information* | *Low* | *Low* | *Low* |  |  |  |  |
| *C.3.1.2 – Help desk services* | *Low* | *Low* | *Low* |  |  |  |  |
| *C.3.4.4 – Services acquisition* | *Low* | *Low* | *Low* |  |  |  |  |
| *C.3.5.1 – System development* | *Low* | *Moderate* | *Low* |  |  |  |  |
| *D.20.2 – General purpose data and statistics* | *Low* | *Low* | *Low* |  |  |  |  |
| *D.21.1 – Inspections and auditing* | *Moderate* | *Moderate* | *Low* |  |  |  |  |
| *C.2.6.1 – Customer services* | *Low* | *Low* | *Low* |  |  |  |  |
| *C.2.3.4 – Strategic planning* | *Low* | *Low* | *Low* |  |  |  |  |

# This page left intentionally blank

# Appendix B: Digital Identity Worksheet

***Instruction:*** *Complete the digital identity worksheet table below table below*

**Mapping impact Levels to NIST SP 800-63 Levels**

Digital identity is the process of establishing confidence in user identities electronically presented to an information system. Authentication focuses on the identity proofing process, the authenticator management process, and the assertion protocol used in a federated environment to communicate authentication and attribute information, if applicable.

Table A.1, below, “Mapping Levels to NIST SP 800-63 Levels”, maps the impact levels to NIST SP 800-63 Digital Identity Guidelines levels:

* Identity Assurance Level (IAL) - Refers to the identity proofing process
* Authenticator Assurance Level (AAL) - Refers to the authentication process
* Federation Assurance Level (FAL) - Refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable), to a relying party (RP)

### Table B.1

| **Impact Level** | **Identity Assurance Level (IAL)**  **Authenticator Assurance Level (AAL)**  **Federation Assurance Level (FAL)** | **Identity Assurance Level (IAL)**  **Authenticator Assurance Level (AAL)**  **Federation Assurance Level (FAL)** | **Identity Assurance Level (IAL)**  **Authenticator Assurance Level (AAL)**  **Federation Assurance Level (FAL)** |
| --- | --- | --- | --- |
| **Moderate** | IAL2: In-person or remote, potentially involving a “trusted referee” | AAL2: Multi-factor required; authenticators and verifiers use FIPS 140-validated cryptography | FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it |
| **Low** | IAL1: Self-asserted | AAL1: Single-factor or multi-factor; verifiers use FIPS 140-validated cryptography | FAL1: Assertion is digitally signed by the identity provider |

### 