Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

General Information

PIA Identifier: 465
System Name: Enterprise Document Management System (EDMS)
CPO Approval Date: 7/12/2024
PIA Expiration Date: 7/12/2027

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

John Hartbarger

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Enterprise Document Management System (EDMS)

B: System, application, or project includes information about:
Federal Employees, Contractors, the public

C: For the categories listed above, how many records are there for each?
PII Data for each System that have documents stored in EDMS.

STR - 652,224

TAMS - 504,012

EASI - 7,447,273

OGE - 41,504

D: System, application, or project includes these data elements:
SSN, Personal Email Address, Home Address, Home Telephone Number, Taxpayer Identification Number (TIN), Mobile Phone Number, Driver's License Number, Employment Information.

Overview:

The purpose of the Electronic Document Management Software (EDMS) system is to serve as a repository for GSA documents to reduce paper storage and provide reliable and secure access to documents where and when they are needed. The information system also allows for Enterprise document management and records management functionality.

The nature of the data stored in EDMS is of ‘finished’ documents produced by GSA and that will be declared as Records. The EDMS stores PII data but does not store PCI or authentication data. The application is on-premises, will be accessed by authorized internal GSA and will not be available outside the GSA Domain. The following types of PII may be collected by the system:

The STR system collects individuals name, home address, Taxpayer Identification Number (TIN) and Driver's License Number.

The TAMS system collects individuals name, SSN, Home address, and Taxpayer Identification Number (TIN).

The EASI system collects individuals name and Taxpayer Identification Number (TIN).

The OGE eForm system collects individuals name, personal email address, home address, home telephone number, mobile number and employment information (.e.g. previous employment).

The EDMS application has two user sets that transact and access via different authentication methods. The first is the GSA Front End user set, the other, Privileged Accounts, are reserved for those users with an active SNA and have been granted permission to access the EDMS on the application back-end level.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
EDMS ensures that GSA meets the Managing Government Records Initiative (M-12-18) and the Federal Property and Administrative Service Act as amended (40 U.S.C. Sec.585).

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
EDMS is currently under the GSA/PBS- 8 (Electronic Document Management System - EDMS). The information is searchable via full-text search, but will only be returned in a search result if the person has been permitted access by the business line.

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
Alfresco contains a Records Management module that has the NARA-approved records schedules configured with cutoff date rules, retention periods, descriptions, retention authorities, and dispositions. As content is migrated into the EDMS, it is tagged with both a record schedule and (if available) a cutoff date when the content is “closed” or completed. That cutoff date is used to calculate the built-in retention period for keeping it until scheduled for disposal. EDMS content eligible for disposal is reviewed in the first quarter of each year, and either destroyed with concurrence from the participating business line, disposed of after review by a GSA Senior Records Officer, accessioned to NARA as a permanent record, or retained as a business reference copy for the business line for a stated period of one year until the next review period.
EDMS adheres to the GSA 1820.2
Retention Instructions: Cutoff at the end of the fiscal year when destructions are completed. Keep for 20 years or until no longer needed for business purpose, whichever is later.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? No

2.1 Explain: If not, please explain.
EDMS serves as a back end source system that collects PII, therefore, the business systems will/are responsible for the PII user notice when they collect. Business lines own the source initially submitted by respondents and are informed legally when they submit their information.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
EDMS provides a secure, encrypted, non-public environment with strict controls around site, folder, and document access. EDMS serves as the GSA Enterprise repository of documents for integrating systems that may have unique business needs to store PII as the document originators. EDMS places all stored documents on a Records Management schedule, where they are stored only as long as legally required per their assigned GSA Record Category, and then permanently disposed of unless categorized as permanent records.

3.2: Will the system, application, or project create or aggregate new data about the individual?
No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
Organization users (Internal) of EDMS consist of GSA employees and contractors. EDMS does not have any Non-organizational users. Account provisioning is handled through EDMS and the GSA’s Enterprise Active Directory. A user’s privileges are based on their group/role, as determined by the Business Manager submitting the user account

request. Site and folder level access are limited since users are identified by the business in defined roles. Organization users in EDMS must participate in the GSA security and privacy training, as part of GSA IT mandated policy for users accessing internal systems and information.

3.4 Will the system monitor the public, GSA employees, or contractors?
GSA Employees

3.4 Explain: Please elaborate as needed.
The system only monitors those users (GSA employees and contractors only) who access the system directly. In the case of integration with another system EDMS logs the interaction with the system account, the source system would be the system of record of the end user

3.5 What kinds of report(s) can be produced on individuals?
EDMS does not provide users the ability to generate reports on individuals; it is simply a document repository application

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?
EDMS does not provide users the ability to generate reports on individuals. Depending on their level of access, a user will only be able to access content that they are authorized to access.

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
None

4.2How: If so, how will GSA share the information?
EDMS does not share any information with any individuals, federal/state agencies or private sector organizations. Only FOIA requests are fulfilled as needed.

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
EDMS does not collect any personal information directly from end-users or store personal information in internal database fields. EDMS does allow end-users to upload documents without system restrictions on the content of those documents. Documents known to intentionally contain PII are sent from other GSA systems to EDMS via system interfaces. EDMS interacts with EASI, GREX, OGE, Salesforce, Kahua, and Mulesoft.

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
Yes

4.4WhoHow: If so, who and how?
The EDMS system does not interact with external systems outside the GSA domain. EDMS does interact with internal systems within the GSA domain utilizing Alfresco Content Management Interoperability Services (CMIS) APIs and EDMS service accounts. This integration allows the pushing and pulling of documents to and from their

connected EDMS folders. Access is controlled by service accounts and group permissions within EDMS. EDMS interfaces with additional systems that do not process or store PII.

4.4Formal Agreement: Is a formal agreement(s) in place?
Yes

4.4NoAgreement: Why is there not a formal agreement in place?

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
EDMS does not perform any data manipulation or validation of completeness. EDMS provides the information in the database as read only.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Organization users (Internal) of EDMS consist of GSA employees and contractors. EDMS does not have any Non-organization users. Account provisioning is handled through EDMS and the GSA's Enterprise Active Directory. A user's privileges are based on their group/role, as determined by the Business Manager submitting the user account request. Site and folder level access are limited since users are identified by the business in defined roles. The content in EDMS is organized in Sites that are restricted to users and permissions determined by the business owner of each site to both meet their business needs and establish controlled access to content that may contain sensitive or controlled information. This approach can also be applied at a more granular level applying access restrictions to folders and folder hierarchy to further restrict access to content. Business site owners and integrated applications establish site and folder level access strategies to fit their security needs. The security restrictions include access as well as ability to search content. Organization users in EDMS must participate in the GSA security and privacy training, as part of GSA IT mandated policy for users accessing internal systems and information.

6.1b: What is the authorization process to gain access?
GSA users undergo its on-boarding and access approval process. All GSA users for EDMS project undergo regular GSA background check and onboarding process, where all necessary GSA approvals occur.

Application Accounts: New accounts creation includes the following steps:
1. New on-board has been given preliminary approval by GSA through GSA background investigation process.
2. Employee in coordination with their respective Team Lead requests access to appropriate applications, tools, databases, and/or environments using Access Request Form.
3. Team Lead provides approval of the new access based on employee job role.
4. The new user request is imitated by a manager to the EDMS team. This request must include role and access, based on guidance from the supervisor. The supervisor is responsible to approve that it is a valid request. The program manager is responsible for verifying that the user does need the permissions requested based on their job responsibilities.
5. Finally, GSA implements Active Directory groups throughout the enterprise infrastructure. Active Directory groups are the preferred methodology for providing access to GSA resources. Domain user accounts (Long name accounts) and SNA accounts are added to AD groups as necessary after access request reviews and approvals.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
3/31/2024

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
EDMS has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ a variety of security measures defined in the System Security Plan (SSP) designed to ensure that information

is not inappropriately disclosed or released. A user's privileges are based on their group/role, as determined by the Business Manager submitting the user account request. The encryption undertaken by EDMS is FIPS (Federal Information Processing Standards) compliant which ensures that PII is encrypted when uploaded or transmitted to, and when stored in EDMS. Metadata and property information stored in all EDMS databases are encrypted. Binary files (documents) are encrypted and stored in the Alfresco content store. The content store uses symmetric encryption to encrypt the document before it is written to the content store. In addition, the Solr search drives are also encrypted. EDMS users access the Alfresco backend repository via the EDMS system frontend or web service call utilizing an HTTPS (secure internet) connection using a CA (Certificate Authority) signed certificate, which ensures secure HTTPS connection.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: What are they?
The EDMS staff follows process outlined in the GSA Incident Response Procedural Guide (CIO IT Security 01-02) to report and respond to any identified security incidents pertaining to PII.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
EDMS does not solicit any information from individuals.

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
EDMS does not solicit any information from individuals.

7.2: What are the procedures that allow individuals to access their information?
Should an individual request access to their information, it would be through specific business lines who would have access to EDMS for their own business repository and not the whole
system

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
The GSA Information Technology (IT) Security Policy CIO P 2100.1 requires GSA associates and contractor personnel to complete security and privacy awareness training annually. New and returning GSA employees and contractors must complete the basic security awareness training and privacy training within thirty (30) days of employment.

The training is administered through GSA's Online University site. This training requires electronic acknowledgement when the employee has completed the course. Per the GSA Information Technology (IT) Security Policy CIO P 2100.1, if an employee or contractor does not complete the training during the thirty (30) day training period, their GSA e-mail access is immediately terminated. The EDMS PM coordinates with users and contractor personnel to ensure that all users complete the annual online IT security and privacy training course entitled, GSA Security and Privacy Awareness Training.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?

All content stored within EDMS is encrypted and access to folders and sites are controlled by roles and permissions assigned by the primary and secondary owners of an EDMS site. Primary and secondary owners are assigned the role of site manager. Periodic update and review of this PIA will be conducted once new team developers, business line team members, or future engagement stakeholders are onboarded. Integrated access is typically managed through service accounts and business lines determine how documents, user groups, roles, and permissions are controlled on the site. In addition, EDMS has an audit capability which monitors user activity (logins, deletions, updates, etc.). An EDMS user role determines what a user can access within the site. Each role has a default set of permissions and site managers determine the access granted to users for their managed sites. The EDMS tech team implements and updates user roles only with site manager approval. Managers have full rights to all site content - what they have created themselves and what other site members have created. Collaborators have full rights to the site content that they own and Contributors can only edit content they own on a site. Consumers are the users with read-only access to documents. All users must have an ENT account and must access EDMS with their ENT credentials. Users will only have access to sites where granted permission by site managers and only for their assigned role.