Privacy Impact Assessment
Management Support Systems (MSS)

Technology, Planning, Architecture, & E-Government

- Version: 1.2
- Date: January 23, 2020
- Prepared for: USDA OCIO TPA&E

USDA
United States Department
of Agriculture

Privacy Impact Assessment for the

Management Support Systems (MSS)

January 23, 2020

Contact Point
Sherry Golden
USDA Digital Infrastructure Services Center (DISC)
816-823-5280

Reviewing Official
Dave Ireland
Director, Security Division, ISSPM
United States Department of Agriculture
816-926-2331

Abstract

The Management Support System (MSS) is an application owned by the Digital Infrastructure Services Center (DISC) Data Center Hosting Services (DCHS). Currently, MSS encompasses two applications: Living Disaster Recovery Planning System (LDRPS) and Internal Technical Information Wiki (Wiki) MSS contains PII limited to USDA employees' home address and in some cases, optional information including USDA employees' emergency contact phone number, which are normally not USDA employees or contractors.

Overview

Management Support Systems (MSS) is owned by the Digital Infrastructure Services Center (DISC) Data Center Hosting Services)   Currently, MSS encompasses two applications: Living Disaster Recovery Planning System (LDRPS) and Internal Technical Information Wiki (Wiki). LDRPS is an application to enable users to build, modify, and print disaster recovery plans to help DISC and DISC DCHS recover its information systems, should a disaster occur. Wiki is a collaborative internal website that aggregates the collective work of internal users. MSS is not specifically marketed rather it provides support services to DISC, DISC DCHS, and customer systems. MSS is accredited by the USDA

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1   What information is collected, used, disseminated, or maintained in the system?

- USDA Employees' Personal Phone Number
- USDA Employee Home Address
- USDA Emergency Contact Phone Number

1.2   What are the sources of the information in the system?

Employee Emergency Contact forms.

1.3   Why is the information being collected, used, disseminated, or maintained?

Information collected by LDRPS is used in the event of a disaster that could result in the deterioration or inability to use DISC's facilities or in the event an emergency occurs to a USDA employee located at a DISC facility.

1.4   How is the information collected?

New hires provide contingency management with an emergency contact form.

1.5   How will the information be checked for accuracy?

This is personal information provided by the new employee. It is up to each individual to provide accurate information. DISC does not check data for accuracy.

1.6   What specific legal authorities, arrangements, and/or agreements defined the collection of information?

No legal authorities, arrangements, and/or agreements have been set forth to define the collection of information within Management Support System. Any and all information collected is entered by, and with the full responsibility of the individual.

1.7   <u>Privacy Impact Analysis</u>: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy risk is extremely low. Only two DISC DR coordinators have access to LDRPS and the information is only release to management upon request.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1   Describe all the uses of information.

Information collected by LDRPS is used in the event of a disaster that could result in the deterioration or inability to use DISC's facilities or in the event an emergency occurs to a USDA employee located at a DISC facility

2.2   What types of tools are used to analyze data and what type of data may be produced?

There are no tools to analyze the data. It is stagnate data and only updated upon employee request.

2.3   If the system uses commercial or publicly available data please explain why and how it is used.

Information is not commercially or publicly available.

2.4   **Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.**

The LDRPS software is accessed through the NAG and only the DR Coordinators have access to the software.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1   **How long is information retained?**

Information is retained for the duration of an individual's employment with USDA/DISC.

3.2   **Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?**

No.   This is stagnate data and only kept as long as the employee is employed by DISC

3.3   **Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.**

Unintended exposure or breach of information contained on LDRPS could expose personal information to unauthorized individuals.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1   **With which internal organization(s) is the information shared, what information is shared and for what purpose?**

Information is not shared outside of USDA/DISC.

4.2   **How is the information transmitted or disclosed?**

Information is not transmitted to any other systems or entities outside of the USDA/DISC. Information is not disclosed to anyone outside of those authorized to view the information through DISC RBAC access controls.

4.3   Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The risk of unintended information sharing is restricted through access controls governed by the DISC RBAC access process and associated controls.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1   With which external organization(s) is the information shared, what information is shared, and for what purpose?

Information from LDRPS is not shared with external organizations.

5.2   Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Information from LDRPS is not shared with external organizations.

5.3   How is the information shared outside the Department and what security measures safeguard its transmission?

Information from LDRPS is not shared with anyone outside of DISC. Additionally, information contained within LDRPS is limited to those with access governed by the DISC RBAC process and associated controls.

5.4   Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Information from LDRPS is not shared with external organizations.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1   Was notice provided to the individual prior to collection of information?

Yes.

6.2   Do individuals have the opportunity and/or right to decline to provide information?

Yes.

6.3   Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Yes. Individuals are asked, but it is not required to complete the Emergency Contact Form which is sent to the DISC CMT team.

6.4   <u>Privacy Impact Analysis</u>: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Individuals within DISC are provided Emergency Contract Form to fill out to provide emergency contact information. This form is not required to be completed. Individuals can opt out of completing the form and/or certain sections of the form they do not want to share.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1   What are the procedures that allow individuals to gain access to their information?

Employee   Requests   copy   of   information

7.2 **What are the procedures for correcting inaccurate or erroneous information?**

Employee contacts the Contingency Management Team to make corrections.

7.3 **How are individuals notified of the procedures for correcting their information?**

They just send the Contingency Management team and email.

7.4 **If no formal redress is provided, what alternatives are available to the individual?**

Employee contacts the Contingency Management Team to make corrections

7.5 **Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.**

There are no risks

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 **What procedures are in place to determine which users may access the system and are they documented?**

DISC follows SOI 7-7 LDRPS Account Management for managing accounts

8.2 **Will Department contractors have access to the system?**

No

8.3 **Describe what privacy training is provided to users either generally or specifically relevant to the program or system?**

All DISC Employees are required to complete on an annual basis, and prior to gaining access to any USDA system upon hiring, the USDA Security and Awareness training.

8.4   Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes, certification & accreditation is completed by the USDA. MSS was originally accredited in 2010.

8.5   What auditing measures and technical safeguards are in place to prevent misuse of data?

Account Registration, Role Authorization, Permission/Role Changes, Approvals within the application, account activity within the application, authentication events, session timeout and session termination.

8.6   <u>Privacy Impact Analysis</u>: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Unintended exposure or breach of information contained on LDRPS could expose personal information to unauthorized individuals. This is mitigated through access processes and associated controls.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1   What type of project is the program or system?

Application hosted on the DISC Midrange platform.

9.2   Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

n/a – there are no third-party websites. The software is on DISC owned servers.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

n/a

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

n/a

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

n/a

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

n/a

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

n/a

If so, is it done automatically?

n/a

If so, is it done on a recurring basis?

> n/a

10.7 **Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?**

n/a

10.8 **With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?**

n/a

10.9 **Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?**

n/a

10.10 **Does the system use web measurement and customization technology?**

n/a

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

n/a

10.11 **Does the system allow users to either decline to opt-in or decide to opt-out of of all uses of web measurement and customization technology?**

n/a

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

n/a

10.12 <u>**Privacy Impact Analysis**</u>**: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.**

n/a

Responsible Officials

Dave Ireland
Director – Security Operations Division, ISSPM
Digital Infrastructure Services Center
United States Department of Agriculture

Edward Reyelts
Authorizing Official
Associate Chief Information Officer (ACIO)
Digital Infrastructure Services Center
United States Department of Agriculture

Victoria Turley
System Owner
Director – DISC Data Center Hosting Services
Digital Infrastructure Services Center
United States Department of Agriculture

Approval Signature

_____

Dave Ireland
Director – Security Operations Division, ISSPM
Digital Infrastructure Services Center
United States Department of Agriculture

_____

Edward Reyelts
Authorizing Official
Associate Chief Information Officer (ACIO)
Digital Infrastructure Services Center
United States Department of Agriculture

_____

Victoria Turley
System Owner
Director – DISC Data Center Hosting Services
Digital Infrastructure Services Center
United States Department of Agriculture