Human Resources Information System Access Request Document

Personal Data – Privacy Act of 1974

Public Law 99-474 (Counterfeit Access Device and Computer Fraud and Abuse Act of 1984) and Public Laws 93-579 (Privacy Act of 1974), authorizes collection of this information. The information will be used to verify that you are an authorized user of a Government automated information system (AIS) and/or to verify your level of Government security clearance. Although disclosure of this information is voluntary, failure to provide the information may impede or prevent the processing of your requested User Account. Records or the information contained therein may be specifically disclosed outside the US Forest Service (FS) generally permitted under 5 U.S.C.552a (b) of the Privacy Act.

Instructions: This document is for employees who need access to Human Resources information systems based on the official duties outlined by their position description. *Every HR employee who needs the various required accesses will complete this document with their supervisor.* ***If supervisors are requesting access for Non-HRM employees, they will need to provide the employees official duties and justification in Section D.***

Initial Access: This document must be completed by both the employee and supervisor. Attach completed document to a HR Help case when requesting elevated accesses and submit case.

Modified Access: This document must be completed by both the employee and supervisor. Attach completed document to a HR Help case and submit case.

Annual Recertification: To continue the Human Resources Information Systems Access, both the employee and supervisor must complete this document. Email completed document to the hrm_system_access@usda.gov mailbox.

> The Annual Recertification and any required AgLearn courses must be completed by the announced date of the respective calendar year.

Remove Access: Complete only Sections A, B, and D. Attach the completed document to an HR Help case and submit case.

NOTES: Employee and supervisor must sign this document with either electronic or wet signature. Employee and supervisor are advised to save a signed copy for their records. This document will be retained for audit purposes.

This document is required to access Human Resources information systems in order to complete "Official Duties" of your position.

Section A: Type of Request: Select only one

☐ Initial Access ☐ Modify Access ☐ Recertification of Access ☐ Remove Access

Section B: Employee Information: All fields in this section are required

1. Employee's Printed Full Name: _____

   Employee's Occupational Series:_____

2. From the AD-332, Master Record/Individual Position Data page, Section C: Individual Position, Box 4: PosSens/Computer/Drug, the 3 character code: ____

3. Training Requirements:
   a. If the employee did not complete the USDA Information Security Awareness training as a new employee via current process, they must complete the training and have it annotated in their AgLearn account before access can be requested/granted.
   b. There may be additional AgLearn training covering Privacy Awareness and Protecting Personally Identifiable Information that must be completed by the announced date of the respective calendar year.

Section C: Employee's Acknowledgement of Understanding and Responsibility

- I certify that all information provided is accurate to the best of my knowledge.
- I agree to comply with training requirements as outlined in FS policy pertaining to PII, Sensitive Information and/or Role-Based Security Training.
- I understand any unauthorized or improper use of accesses and privileges may result in removal of these accesses
- I understand the need to safe guard all PII and Sensitive Information.
- I will not share my User IDs (log in name) or passwords with anyone.
- I will not disclose any PII, sensitive, classified or compartmented information I access or learn of as a result of my privileged user duties and activities without authorization. I will only disclose information with those who have an official need to know.
- I will protect government-issued computer equipment and all portable electronic devices assigned to me at all times. I will not leave government-issued computer equipment exposed in a parked car or any other unsecured location where it might be seen and/or stolen.
- I will not use personally-owned or non-FS issued devices to store government related work.
- I will not use my privileged user access to obtain information or data for which I am not specifically authorized, or for non-official purposes. I further understand that investigation and monitoring of my privileged user activities may be conducted to ensure integrity of agency systems.
- I will collect PII only if required to do so by law or regulation. When required, I will collect the minimum amount of PII required to accomplish my official duties, and delete PII from the hard drive or other electronic device where it is stored when no longer

needed.

- I will ensure appropriate and authorized encryption software is installed on all government-issued computers and devices assigned to me. This includes any government-issued external hard drives and USB flash drives.
- When electronic transmission or physical transport of PII is necessary, I will apply additional protection measures. I will encrypt or password protect any electronic communication or portable media that contains PII. I will double wrap any documents that must be transported through a certified delivery service, and obtain tracking information to confirm delivery.
- I will make paper copies of PII only if it is absolutely necessary to perform official duties. I will not store paper copies of PII at my residence or authorized telework location without the knowledge and approval of my supervisor. I will store paper copies containing PII in a secure, locked cabinet or other locked storage container. I will discard paper copies according to Forest Service policy.
- I have read the USDA's Rules of Behavior included in the annual Information Security Awareness Training, and fully understand my responsibilities and the activities and behaviors that are prohibited.
- I will immediately report to my supervisor and USDA Cybersecurity any incident where PII or other sensitive agency data may have been lost, stolen, or compromised. This includes any suspicious activity I observe by others. USDA Cybersecurity can be contacted at (866) 905-6890, or by emailing cyber.incidents@usda.gov. More information on PII incident reporting can be found on the CIO website: *https:// fsweb.wo.fs.fed.us/cio/cyber-security/contacts-incident-reporting.*
- I will exercise sound judgment and the highest ethical standards when performing duties that require handling and protecting PII and other sensitive/confidential information.

I fully understand and acknowledge the statements listed above. Failure to comply with these responsibilities may result in corrective action, including, but not limited to, formal discipline up to removal from federal employment and/or suspension of system privileges. I further understand any willful disclosure of PII to any person or agency not entitled to receive such information may result in possible criminal prosecution and a fine up to $5,000.

Employee Signature: _____

Date: _____

Section D: Supervisor's Acknowledgement of Understanding and Responsibility

1. Is the employee on a detail or temporary promotion?
   ☐ Yes (If yes, provide the Not To Exceed (NTE) Date of the detail or temporary promotion?)

   ☑ No

   NOTE: The employee's system access will be set to expire on the NTE date. If the detail or temporary promotion NTE date is extended, a new request will need to be submitted.

2. Is the employee an HRM employee?

   ☐ Yes (If yes, which HRM Staff is the employee assigned to? E.g., Pay, Fire Hire Team, Temporary Employment, etc.)

   ☑ No (If no, provide official duties, systems employee needs access to, and specific justification explaining why the Non-HRM employee needs the access requested below.)

   Request elevated access in eMedical to preform my assigned duties.

Acknowledgement of understanding and responsibilities:

- This employee requires HR information system access to perform the official duties of their position.
- It is my responsibility to ensure this employee completes all required AgLearn training and notifies the HRM Privacy Officer once the training is complete to ensure accesses granted are not removed.
- I certify that I have discussed with the employee the need to safe guard all PII and Sensitive Information.
- I certify that I have discussed with the employee that any unauthorized or improper use of accesses and privileges may result in removal of these accesses.
- It is my responsibility to notify the HRM-HRIS section when this employee no longer requires HR Information System accesses. **NOTE:** See instructions at beginning of document to Remove Accesses.

I fully understand and acknowledge the statements listed above. Failure to comply with these responsibilities may result in corrective action, including, but not limited to, formal discipline up to removal from federal employment and/or suspension of system privileges. I further understand any willful disclosure of PII to any person or agency not entitled to receive such information may result in possible criminal prosecution and a fine up to $5,000.

1. Access start date for Employee listed above: _____
2. Supervisor's printed full name: _____
3. Supervisor's signature: _____
4. Date: _____

Section E: Information System Security Officer Statement

In accordance with NIST 800-53 Rev 4, Privileged Profile Review, as required by Controls AC-2, IA-2, and IA-4, are reviewed and approved by the Information System Security Officer on a Quarterly Basis.

Section F: For HRIS Use Only

The boxed checked below indicates which HRM Staff the employee is assigned to. In turn, this correlates to the accesses granted in the FS ConnectHR application and any other applications used to support outside Agencies.

☐ AgLearn Team
☐ Benefits & Retirement
☐ Contact Center
☐ DMAT Team
☐ DQM Team
☐ Drug Testing
☐ HRIS Admin (9)
☐ HRIS Applications Developer
☐ HRIS Student Interns/Staff
☐ HRM Internal Operations
☐ HRM Management
☐ Nat. Fire Hire Team
☐ Nat. Collective Hiring Team
☐ Nat. Temp Employment
☐ PAR
☐ Pay Section
☐ Perf. & Awards
☐ Personnel Security Section
☐ Policy
☐ Public Affairs Office
☐ Employee Relations
☐ Labor Relations
☐ Misc. ER/LR Staff
☐ Staffing/Classification
☐ Suitability
☐ System Admin HRIS (10)
☐ Training & Employee Development
☐ Workers' Compensation Unit
☑ Other: eMedical