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 and non-FS employees who need access to Human Resources information systems based on the official duties outlined by their position description. Every user who needs the various required accesses is required to complete this document with their supervisor or sponsor. If access requested is for Non-HRM employees, provide the employees official duties and justification in Section D. Once the request form is completed and signed by the employee and supervisor or sponsor, the supervisor or sponsor should create a new case in HR Help case and attach the completed System Access Request and any other applicable documents. A job aid is here.

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

Revised: June 6, 2024

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

Last Name: _____ **First Name:** _____ **Middle Initial:** _____

Employee's Occupational Series/Position Title: _____

Organizational Code: _____ **Unit Name:** _____

2. From the AD-332, Master Record/Individual Position Data page, Section C: Individual Position, Box 4: PosSens/Computer/Drug, the 3-Character code: _____
   The AD-332 can be found in your electronic Official Personnel Folder (eOPF) or your eTracker hire, reassignment, or promotion SF52 request.
3. Per Forest Service Manual 6683.61, it is mandatory for users requesting elevated access to complete the Information Security Awareness (ISA) training for the current fiscal year. Completion will be verified, and access will not be granted until completed. Please enter the completion date for your training.

Information Security Awareness Training Completion Date: _____

Section C: Employee's Acknowledgement of Understanding and Responsibility

- I certify that all information provided is accurate to the best of my knowledge.
- I understand any unauthorized or improper use of accesses and privileges may result in removal of these accesses
- I understand the need to safeguard 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 system.

- 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 storage devices.
- 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 storage devices.
- 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 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: Contacts for 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.

The penalty for an employee found guilty of falsification of a payroll document for personal gain is subject to removal (DPM 751, Appendix A). If convicted in a court of law, the individual is subject to a fine of not more than $10,000 or imprisonment of not more than 6 years, or both.

Timesheets are considered to contain personally identifiable information and, in some cases, private health information (PHI). I understand that the violation of certain laws, such as Public Law 99-474 (Counterfeit Access Device and Computer Fraud and Abuse Act of 1984) and Public Laws93-579 (Privacy Act of 1974) or any willful disclosure of PII to any person or agency not entitled to receive such information, may result in possible criminal prosecutions and a fine up to $5,000.

Employee Signature: _____

USDA Email Address: _____

Section D: Supervisor's Acknowledgement of Understanding and Responsibility

1. Is the employee on a detail or a temporary promotion? Yes ◯ No ◯ If Yes, NTE Date
2. Is this an HRM Employee?

◯ Yes (If yes, which HRM Staff is the employee assigned to? E.g., Pay, Fire Hire Team, Temporary Employment, etc.). If you need access to LERIS or EPS, please provide the role(s) needed.

◯ 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).

All Supervisors must complete the justification for their employee. Briefly describe the tasks they will perform with elevated system access. **Examples: Submit or modify T&As for employees in the field in their absence, correct job codes, etc**. See the Justification Guidance for Paycheck8 Elevated Access Requests document for specific justification.

Justification for why the employee needs this access:

Paycheck8 Elevated Access Roles and Responsibilities

Please ***ONLY*** fill out this Paycheck8 section if you are requesting elevated Paycheck8 access.

Paycheck8 Access Type (Select One):

◯ Regional Super User

◯ Regional Read Only

◯ Agency-Wide Read Only (HR and B&F Only)

◯ Pay and HRIS Employees Only

1. **Do not provide copies or information on employees' Time and Attendance (T&As) records when adverse action is being taken against the employee. The requestor will be required to submit a FOIA request or forward his/her inquiry through Employee Relations or Labor Relations.**
2. Only access, modify, or submit T&As you are authorized to service for your region, station, or area.
3. Authorized access should only be granted when an employee is unable to act on his/her own behalf (i.e., emergency/fire assignments, YCC, systemic issues). Do not provide access when adverse action is being taken.
4. When assisting employees', please make sure the profile information located in the Personal Information section has been updated with the employee's current information. This would include contact point, job code, override code, and work schedule.
5. Submit T&As in accordance with NFC's Time and Attendance Instructions. If you are submitting corrected T&A that changes annual or sick leave, monitor leave balances to make sure corrections occur the following pay period. If corrections are not made the following pay period, a leave audit will have to be requested. Any corrected T&A that has credit hours or compensatory time will require a leave audit and will not be automatically updated.
6. Run Paycheck8 reports when requested as part of your duties.
7. Please keep in mind the penalty for an employee found guilty of falsification of a payroll document for personal gain is removal (DPM 751, Appendix A). If convicted in a court of law, the individual is subject to a fine of not more than $10,000 or imprisonment of not more than 6 years, or both.

If an SF-52 was submitted to correct a personnel action but the action was not processed or updated in NFC, have the employee or supervisor open an HR Help case by calling 877-372-7248 and select option 2.

Acknowledgement of understanding responsibilities:

- This employee requires HR Information System access to perform the official duties of their positions. It is my responsibility to ensure this employee completes all required AgLearn training.
- I certify that I have discussed with the employee the need to safeguard 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, suspension of system privileges, or both. 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 about:
2. Supervisor's full printed name:
3. Supervisor's signature:

Section E: Information System 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

HRIS Administrators: Use the dropdown menu's below to select the role(s) granted. If the access needs explanation or if the access granted is different that the roles available in the drop down boxes, please use the text box below to describe the access given.

Note: To select multiple items, press control + left mouse click. Be sure to press enter once selections from a menu have been made, so they appear in the selection box.

Standard Roles	Limited Roles	Contractor Roles
none	none	none
ACE Team (4)	Delete Role	GDCII ADMIN (10)
Aglearn Team (8)	Override Least Privilege	GDCII User(9)
B&F and Travel (4)	ePM - ER Policy (ER Elevated)	Contractor (8) - eMedical Administrator
Benefits & Retirements (4)	ePS	Contractor (8) - LERIS
Contact Center (7)	ER Dashboards (9)	* Contractor (4) - Anti-Harassment
DASI Team (4)	eSafety - InfoSec	* Contractor (4) - Benefits
Drug Testing (4)	Harassment Reporting	* Contractor (4) - Classification
eMedical Sys Admin and Auth (8)	Performance Management ePM Policy	* Contractor (4) - eOPF Team
none	none	none

Notes: