



United States Department of the Interior

FISH AND WILDLIFE SERVICE
Washington D.C. 20240

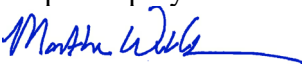


In Reply Refer To:
FWS/AIRT-Dep/076448

February 16, 2022

Memorandum

To: Service Directorate

From: Principal Deputy Director Exercising the Delegated Authority of the Director


Subject: U.S. Fish and Wildlife Service Employee Privacy Responsibilities

The Service collects, uses, and shares personal information from many private and public individuals to fulfill our mission. Safeguarding this information is a shared responsibility of all employees and helps to ensure the public's trust in our agency. As we have experienced over the last two years of increased virtual work and the mandatory collection of health information related to COVID-19, the protection and appropriate handling of privacy-sensitive data is of utmost importance to us all. With the "future of work" getting closer and the implementation of new telework and remote work agreements, please allow me to update everyone on current privacy requirements, employee resources to ensure compliance, and best practices to keep the Service's and your own PII safe.

Section 1-Protecting Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is any information that can be used to identify an individual, including contact information like an email address, phone number, and login or username. PII may be subject to the Privacy Act and should be shared only with those who have official need to know; however, it does not usually require special protection or handling procedures when sharing with authorized recipients due to the low risk of harm disclosing such PII poses.

Sensitive PII (SPII) on the other hand, is identifiable information that if lost, compromised, or inappropriately disclosed could cause substantial harm to the individual or the Service as a whole and requires special handling to protect it from unauthorized disclosure. Examples of SPII include information like Social Security Numbers (SSNs), credit card or financial account numbers, personal identification numbers (PINs), passwords, certain health and medical information, or employment records like negative performance appraisals or adverse actions.

Service employees and contractors must control access to and the dissemination of all PII in their custody. Protecting PII is accomplished by ensuring file sharing systems like SharePoint have correct privacy settings and sharing permissions; sending Sensitive PII as encrypted or password

protected attachments in email; and practicing vigilance when requested to share your own PII as Federal employees are often targets of phishing, spoofing and other social engineering tactics. These measures help prevent unauthorized users and unintended recipients from accessing or downloading files or folders containing PII. When PII is made accessible to unauthorized recipients outside of and within the Service or Department, it is considered a privacy breach and must be reported in accordance with Section 2 of this memorandum.

Section 2-Reporting Privacy Breaches

A privacy breach is the loss of control, compromise, unauthorized disclosure, or unauthorized acquisition of any PII. It is important to report breaches as soon as possible so that the Service's Breach Response Team can lead the breach response as appropriate. Most breaches that do not involve Sensitive PII are considered low risk and do not require notification or offers of credit monitoring to impacted individuals; however, even breaches of non-sensitive PII should be reported in accordance with DOI policy and OMB regulations.

- Report a suspected or confirmed compromise of PII immediately to FWHQ_IRTM_Security@fws.gov or call the Helpdesk at 1-800-520-2433.
- You may also report breaches directly to the Service's Associate Privacy Officer (APO) at fws_privacy@fws.gov, or to DOI's Computer Incident Response Center (CIRC) at DOICIRC@ios.doi.gov or 703-648-5655.

Section 3-Training

All employees and contractors must complete basic privacy awareness and incident reporting training annually. This is accomplished through the Department's Information Management Technology (IMT) Awareness training. The Service also assigns Role Based Privacy Training (RBPT) annually through DOI Talent to those with significant privacy-related duties or access to SPII like Human Resources staff, Supervisors, Administrative staff, Contracting Officer's Representatives (COR), Law Enforcement, IT System Administrators, Privacy Act Managers and those that work with Privacy Act Systems of Records in accordance with OMB Circular A-130, *Managing Information as a Strategic Resource*.

Section 4-Penalties for Privacy Act Violations

There are consequences, ranging from administrative to criminal, should an employee fail to handle PII appropriately (204 FW 1). Improper or unauthorized release of sensitive and administratively-controlled information or employee records is punishable by written reprimand up to removal (370 DM 752.1). Individuals (employees and members of the public) may bring civil and criminal action against the Service for willful and harmful violations of the Privacy Act with fines up to \$5,000.

Most breaches are inadvertent, caused by human error and pose no to low risk of harm. The Service Associate Privacy Officer (APO) will work with employees and supervisors to make sure that all breaches and privacy complaints or concerns are taken seriously and handled

appropriately. For example, the APO may recommend that a re-offending employee be assigned RBPT, or re-take IMT Awareness Training to maintain their network and systems accesses.

Section 5-Privacy Resources

Information Resources and Technology Management (IRTM) has a dedicated privacy office responsible for implementing the Service's privacy program and assisting employees with all matters related to privacy and PII. The Service's APO and other privacy staff work closely with the IRTM Division of Cybersecurity's Risk Management and Compliance Branches, and with offices like Freedom of Information Act (FOIA), Information Collections Clearance/Paperwork Reduction Act (PRA), Joint Administrative Operations Human Capital Division, and the Department's Privacy Office. Privacy staff also work directly with program and system managers that regularly handle PII from employees and the public.

The Privacy office is available to answer your questions, provide assistance, and direct you to privacy guidance and regulations, as well as the tools and resources that are available to help you meet these requirements. Please send privacy and PII concerns and inquiries to FWS_Privacy@fws.gov or call (703) 358-2273. All Service employees are encouraged to follow the [FWS Privacy SharePoint](#) site and visit the [FWS Privacy Intranet](#) site as well as [DM privacy chapters](#) and [privacy toolkit](#) to find helpful tips and guides like these listed below.

- *File Sharing & Permissions guide for OneDrive and SharePoint*
<https://doimspp.sharepoint.com/sites/BisonConnect/SitePages/File-Sharing-%26-Permissions.aspx?source=/sites/BisonConnect&promotedState=1>
- *Safeguarding PII during COVID-19 Response and Sensitive PII Handling Procedures*
<https://doimspp.sharepoint.com/sites/fws-FF09D00000-future-of-work/SitePages/Safeguarding-Privacy-During-COVID-19-Response.aspx?from=DigestNotification>
- *Safeguarding Personally Identifiable Information*
<https://doimspp.sharepoint.com/:w:/s/doi-imt-services/EX29srYk2htLp2BtKI5F8dsBNtrOJ3MHnNhAET31gNmmQA>
- *Sharing Files with External Agencies & Customers*
<https://doimspp.sharepoint.com/sites/doi-imt-services/SitePages/Sharing-Files-with-External-Agencies-&-Customers.aspx>
- *External Guests and Private Channels with MS Teams*
<https://doimspp.sharepoint.com/sites/BisonConnect/SitePages/External-Sharing-with-Microsoft-Teams.aspx>
- *Microsoft Teams Resources*
<https://doimspp.sharepoint.com/sites/BisonConnect/SitePages/Teams.aspx>
- *Encrypt an email in Outlook (Bison Connect)*
https://doimspp.sharepoint.com/:w:/r/sites/fws-FF10T00000/_layouts/15/Doc.aspx?sourcedoc=%7B04583FF7-0435-44E4-AC70-87FCB43A0058%7D&file=MS%20O365%20Outlook-Encrypting%20an%20Email.docx&action=default&mobileredirect=true&DefaultItemOpen=1