

U.S. FISH AND WILDLIFE SERVICE -- REGION 6

PASSWORD CONTROL DOCUMENT

I, the undersigned Employee, have read and/or been briefed on proper utilization of the passwords provided for access to the system listed below and accept the conditions as stated. I understand that it is my responsibility to protect my password from loss or disclosure and to change it in accordance with system guidelines. I understand that my password may be considered a legal signature and that I may be held accountable for any system activities that occur against it. I also agree to abide by all Rules of Behavior for this system provided by the system owner or manager as a condition of access to the system.

General Information:	
<i>Employee Name (print):</i>	<i>Organization:</i>
<i>Employee Signature:</i>	<i>Date:</i>
<i>Type of employee:</i>	
<i>Supervisor (print):</i>	
<i>Supervisor Signature:</i>	<i>Date:</i>
<i>System to which access is requested:</i>	
<i>Reason for access:</i>	
<i>Level of access requested:</i>	
Access Approval by System Owner or Manager	
<i>Name:</i>	<i>Organization/Title:</i>
<i>Signature:</i>	<i>Date:</i>
<i>Comments:</i>	
Termination of Access	
Employee	System Owner or Manager
<i>Date:</i>	<i>Date:</i>
<i>Signature:</i>	<i>Signature:</i>

Instructions: This form is required by Service Manual 270 FW 7 and should be submitted for every user who requests access to an Automated Information System that requires user authentication to gain access. Supervisors should fill out and sign the form, have their employee sign, attach a copy of the employee's current "Statement of Responsibility" form, and submit to the system manager for approval. The system owner or manager should provide the user with any system-specific Rules of Behavior. Upon approval of the application, the system owner will provide a copy of the password control document to the user's Regional Information Technology Security Manager (RITSM). When access to a system is no longer required, including transfer or departure of an employee, the supervisor will notify the RITSM, who will in turn notify the system owner of each system for which that employee has a system application on file. System owners and RITSMs will enter on this form the date that access was removed and retain the information for one year.