PERSONAL COMPUTER USE AGREEMENT - EMPLOYEE CERTIFICATION

(*Original to be attached to and filed with the property pass - copy to be provided to employee*)

The use of government computers at home is a privilege. Such computers are primarily for Government use but may be employed for personal use to a *limited degree.* Employees should ensure that they adhere to the following guidelines regarding the use of such computers at home -- in order to protect themselves and the agency from any unnecessary litigation.

Appropriate General Use:

- Limit use of government computers for personal reasons.
- Limit visits to websites that are not related to your job, career, or continuing education.
- Avoid websites that are inappropriate, or which may be adversarial to the mission of the bureau.
- Do not use email to represent the agency in any manner not appropriate with one's position and for which one has not received proper clearance.
- Generally, do not transfer, maintain or store work material on a home *personal* computer. This may cause problems when answering or processing FOIA and Privacy Act requests for such information.

FOIA:

- Segregate personal records from government records (in order to ensure ease of processing should we receive a FOIA request for information stored on such computers). *Remember*: Government computers used at home are subject to the FOIA.
- Apply the same review, approval, and appeal procedures required by the bureau, Department, and statute should you be working at home on a FOIA or Privacy Act request - whether using a Government or personal computer.

Information Collection:

- Do not collect information from the public (public means any non-Federal employee) *on behalf of the Government* using a *personal* email address or *personal* URL site.
- Do not collect information from the public unless it has been approved by the bureau Information Collections Officer.

Privacy Act Files: *(arranged and generally retrieved by a unique personal identifier such as name, ss#, etc. - such as OPF's*)

- Ensure the proper security safeguards including securing rooms where Government computers are used, appropriate password protections, and positioning the computer in a location not easily accessible or available for use or viewing by the public.
- Remember: You are responsible for the security of the Privacy Act information contained therein, and should use all precautions (such as password protection, removal of Privacy Act information to a separate disk; destruction of any backup copies, etc.) when dealing with Privacy Act files.
- Generally, do not transmit Privacy Act information using email - unless you have a dedicated line (email configuration) set up by ITM. Though such configurations are *more* secure, ITM is required to save backup copies for a period of time. If you do not have a dedicated line set up by ITM, such information may be at risk by sending it to the wrong mailbox or because of backup procedures used by your home Internet Service Providers (ISPs).
- Ensure that any hard-copy (printed) Privacy Act material is secure; and do not fax that material unless you are sending it to those *authorized* to see it and who have a secured fax machine (a fax machine not in open area).
- Do not store or maintain Privacy Act records at home (no secret records). Remember: Specific locations and personnel authorized to maintain such files are identified in the bureau's system of records notice for such systems.

Records Management:

- Retain drafts, and work-related email (created at home in the conduct of agency business) in accordance with the bureau's records schedule (*http://policy.fws.gov/a1283fw2.html*) - as they are agency records and subject to FOIA.

Security:

- Ensure appropriate security (firewalls, virus, and password protection) especially if using email or surfing the Internet. If a file is corrupted - do not transmit it to (or reuse it in) the office.
- Secure the computer at all times - as it is Government property. Do not leave it unattended or in an unsecured place.

I have read, understand, and agree to the above conditions.

_____	_____	_____	_____
(DATE)	**(EMPLOYEE NAME)**	**(EMPLOYEE SIGNATURE)**	**(ORGANIZATION)**