

1a. Employee Name ( <i>Last, First, MI</i> )	1b. Employee Job Title
1c. Department Employed/Detailed	1d. Employee Office Telephone ( <i>Include area code</i> )

2a. Justification for the assignment of a laptop or other portable devices (*Include type of equipment*)

2b. Justification for the storage of sensitive data needed to perform duties of position (*Include type of data*)

**TO BE COMPLETED BY EMPLOYEE:**

I understand that I am required to follow the information security requirements for computing equipment and the data it contains as stated in HBK AS-805-C, Information Security for General Users. <http://blue.usps.gov/cpim/ftp/hand/as805c/welcome.htm>

I understand that I am responsible for the security of this computing equipment and any data that it contains.

I have been issued encryption technology and materials providing training on how to use that technology. I have reviewed these training materials and I understand that I am required to use the Postal Service approved encryption methods outlined in the training to safeguard sensitive data.

I understand that I am required to immediately report any missing or stolen computing equipment as outlined in the USPS Computing Equipment Loss Notification Procedures (dated Oct 2006). [http://blue.usps.gov/caweb/privacy/documents/equiploss\\_notification.rtf](http://blue.usps.gov/caweb/privacy/documents/equiploss_notification.rtf)

I understand that when traveling with computing equipment, I am fully responsible for the security of this equipment. Whenever leaving the computing equipment unattended in either a hotel, residence, duty station or other Postal Service facility, I understand that I must secure this computing equipment. Examples include: Via cable lock issued to me, in a locked safe or locked cabinet.

I understand that in the case of lost or stolen computing equipment, the replacement of such equipment will require approval by my functional Vice President.

**NOTE:** For more information regarding data security please visit the Privacy Office website at: <http://blue.usps.gov/caweb>

<b>Employee Signature:</b> I have read and I understand and I agree to be bound by the above terms of use and for the portable device issued to me.	Date (MM/DD/YYYY)
---	-------------------

**DATA ACCOUNTABILITY APPROVALS**
**Approving Manager**

Yes  No  Employee has permission to have a laptop or other portable media device.

Yes  No  Employee has permission to store sensitive data on computing equipment.

Yes  No  Employee has permission to take computing equipment off Postal Service premises.

<b>Approving Manager (EAS) - Name/Title (please print)</b>	<b>Signature</b>	Date (MM/DD/YYYY)
<b>PCES/Executive - Name/Title (Approval Required) (please print)</b>	<b>Signature</b>	Date (MM/DD/YYYY)

**NOTE:** Provide a copy to the employee and forward the original to the District Information Systems Manager. For headquarters employees, forward the original to Headquarters Computing Infrastructure Services (HCIS).

**Privacy Act Statement:** Your information will be used to process your request to obtain and store sensitive data on U.S. Postal Service™ (USPS®) computing equipment. Collection is authorized by 39 U.S.C. 401. Providing the information is voluntary, but if not provided, we may not process your request. We may only disclose your information as follows: in relevant legal proceedings; to law enforcement when the USPS or requesting agency becomes aware of a violation of law; to a congressional office at your request; to entities or individuals under contract with USPS; to entities authorized to perform audits; to labor organizations as required by law; to federal, state, local or foreign government agencies regarding personnel matters; to the Equal Employment Opportunity Commission; and to the Merit Systems Protection Board or Office of Special Counsel.

# Instructions for Completing PS Form 1357-D

**NOTE:** Print all entries except for signatures. Incomplete information may cause delays in implementation or return of this form.

**Section 1: Employee Information**

- a. Print your full name.
- b. Enter your official job title.
- c. Enter the department where you are employed.
- d. Enter your work phone number.

**Terms of Use Agreement**

- a. Read responsibility statements on encryption, protection and notification procedures.
- b. Sign and date.

**Section 2: Justification of Need**

- a. Describe the job requirements and why the portable equipment is required. Include type of equipment (BlackBerry, laptop, flash drive, etc.)
- b. List the type of Sensitive data being stored and the reason the data is needed to perform the duties of the job.

**Data Accountability Approvals**

- a. Approving Manager: Check the appropriate response to each permission statement; print your name, sign, and date.
- b. PCES Manager, or designee: Review permission statements, print your name, sign, and date.
- c. Provide a copy to the employee.

**NOTE:** Additional information can be found in Handbook AS-805-C, Information Security for General Users and Administrative Support Manual (ASM), sections 22 and 82, both of which are available on Policy Net website at <http://blue.usps.gov/cpim/>. Encryption training, Encryption 101 is available on USPS-TV On Demand.

## Descriptions

**PERSONAL**

Sensitive information includes certain personnel and medical information, court-protected change-of-address requests (COAs), and records protected by legal privileges. Personally Identifiable Information (PII) includes the following data elements and any other personal information which is linked or can be linked to an individual.

The data elements below when by themselves or, linked with other data elements are sensitive:	The following are data elements that when alone, may not be sensitive. However, when linked to other elements in the list, they may become sensitive:
<ul style="list-style-type: none"> <li>Social Security number</li> <li>Driver's license number</li> <li>Credit card number</li> <li>Bank account number</li> <li>Tax ID number</li> </ul>	<ul style="list-style-type: none"> <li>Name</li> <li>Date and place of birth</li> <li>Home or personal e-mail address</li> <li>Home or personal phone numbers</li> <li>Date and place of birth</li> <li>Mother's maiden name</li> <li>Employee ID</li> </ul>

Types of personal information or elements that become sensitive when tied to a person's identity by one or more of the above elements include:	
<ul style="list-style-type: none"> <li>Parental/Marital status</li> <li>Sex</li> <li>Race</li> <li>Religion</li> </ul>	<ul style="list-style-type: none"> <li>Political affiliation</li> <li>Personal assets</li> <li>Biometric records, e.g., fingerprints, etc.</li> <li>Medical records</li> </ul>

**BUSINESS**

There is not a comprehensive list of business data that needs to be protected, as it often depends on the conditions under which the data is exchanged or used within the Postal Service or among business partners. Business data, is data if made public outside of the Postal Service, could harm the Postal Service's business capability or brand, or that of a business partner or customer, such as revenue, mail volumes, or other financial data.

Information describing non-public postal proprietary data or data belonging to customers or business partners is considered sensitive as well, including:	
<ul style="list-style-type: none"> <li>Tax ID numbers</li> <li>Customer or business partner financial data not publicly available</li> <li>Comparative business data such as the amount of business we have among various customers</li> <li>Bank account numbers</li> <li>Asset account numbers</li> </ul>	<ul style="list-style-type: none"> <li>Postal account numbers</li> <li>Information under non-disclosure</li> <li>Contract specific data, e.g., terms and conditions, bid data, or comparative evaluation data</li> <li>Postal restricted information</li> <li>Credit card numbers</li> <li>Proprietary information shared among business partners</li> </ul>

This approval is valid for your current position only. Any reassignment will require a new application for equipment and the storage of data.