

Section 5 - Sensitive Items

I. General Information

A. Definition of Sensitive Item

These are items that are generally for individual use, or that could be easily sold and are most often subject to pilferage or misuse. Sensitive items are:

- firearms and other weapons;
- computers (desktop, tablets, and laptops) including network servers;
- Portable printers, scanners, projectors;
- cellular/smartphones and personal digital assistants (PDA);
- software for internal use with an acquisition cost over \$5,000 and less than \$30,000; and cameras, televisions, and other video equipment with an acquisition cost over \$500 and less than \$5,000.

II. Management and Control of Sensitive Items

A. Procedures For Receiving Sensitive Items

1. Receiving Sensitive Items

a. From Vendors

- 1) Upon receipt of the sensitive item, the person responsible for receiving should examine the shipping container for external damage. If the shipping container is damaged, refer to “Damaged Shipping Container/Damaged Sensitive Items” in the “Handling Unusual Situations” section that follows.
- 2) Open the shipping container and inspect the sensitive item received. If the sensitive item is damaged, refer to the “Damaged Shipping Container/Damaged Sensitive Items” in the “Handling Unusual Situations” section that follows.
- 3) Search for the packing slip. Compare the sensitive items received to the items shipped as reported on the packing slip and note the items received. Sign and date the packing slip. If the vendor did not provide a packing slip, prepare a substitute receipt indicating the items received, and sign and date this document.
- 4) Keep the sensitive items in a secure area, not in an open receiving dock area, to safeguard the sensitive items until they can be delivered to the appropriate location.
- 5) Deliver the sensitive items to its intended location or to the person who requested that the sensitive item be ordered.
- 6) If acceptance testing is necessary, have the person putting the sensitive item into operation sign the packing slip (or substitute receipt) if the sensitive item is in acceptable condition for use. If the sensitive item is unacceptable, refer to the “Handling Unusual Situations” section that follows.
- 7) Provide a copy of the packing slip (or substitute receipt) to the agency inventory coordinator/sub-coordinator as soon as new sensitive items are inspected and found to be acceptable.
- 8) Follow procedures for receiving assets in SWIFT or other approved recordkeeping systems. Additional information can be found in the SWIFT Asset Management [Quick Reference Guides](#).

- 9) Submit the original packing slip (or substitute receipt) to the person responsible for making invoice payments.

b. From Donors

- 1) Follow the gift and acceptance policy for the agency, and Statewide Financial and MAPS Policy - [MAPS Operating Policy and Procedure 0602-12](#), Gift Acceptance.
- 2) Follow procedures 1 through 8 in the section above.
- 3) Submit the original packing slip (or substitute receipt) to the person responsible for acknowledging acceptance of the donated sensitive item.

c. Through an Intra-Agency Transfer – Refer to procedures on page 5-5 of this section.

d. Through an Inter-Agency Transfer – Refer to procedures on page 5-5 and 5-6 of this section.

2. Handling Unusual Situations

a. Damaged Shipping Container/Damaged Sensitive Items

- 1) If there is evidence of external damage, an actual inspection of the sensitive item should be made in the presence of the carrier.
- 2) If the actual inspection of the sensitive item cannot be done, the driver should be required to note that the container was damaged on the agency copy of the packing slip (or substitute receipt), along with the current date and the driver's signature.
- 3) If, upon actual inspection, the sensitive item is damaged, a claim for damage should be submitted to the carrier or the vendor as soon as possible.
- 4) Note on the packing slip (or substitute receipt) that the sensitive item was damaged, and sign and date the packing slip. Send a copy of the original packing slip (or substitute receipt) to the person who requested sensitive item or the agency buyer.
- 5) The person who requested the sensitive item or the buyer should follow-up on the claim by working with the vendor until the claim is resolved.
- 6) Send the original packing slip (or substitute receipt) to the person who processes invoice payments so the person knows the vendor should not be paid until the claim is resolved.
- 7) A [vendor performance report](#) should be sent to MMD-Vendor Management as appropriate.

b. Partial Shipments

- 1) Follow the procedures for receiving sensitive items in 1.a.1 through 1.a.9 above.
- 2) The person who requested that the sensitive item be ordered should follow-up on partial shipments. Discrepancies between provisions of the purchase order and the sensitive item received should be resolved by contacting the vendor as soon as possible.
- 3) Follow-up on unshipped sensitive item ordered until they are received or the order needs to be canceled.
- 4) Cancel the remainder of order if the vendor cannot provide the ordered sensitive item when needed.

c. Fiscal-Year-End Acquisition

- 1) Be sure that the date the sensitive item is received is clearly indicated on the packing slip (or substitute receipt).

- 2) When making the payment, the transaction must be reported in the correct fiscal year which is the fiscal year when the sensitive item was received.
- 3) If the sensitive item acquired on or before June 30 cannot be paid prior to the statewide accounting system's fiscal year end close, follow MMB's annual close instructions for coding the payment to the correct accounting period.

d. Sensitive Item Delivered to Wrong Address

- 1) Contact the carrier or postmaster to deliver the sensitive item to the correct address or to return the sensitive item to the sender.

e. Wrong Sensitive Item Delivered

- 1) Notify the vendor immediately that wrong sensitive item was delivered.
- 2) Make necessary arrangements with the vendor for the return of the wrong sensitive item and delivery of the sensitive item ordered. Authorization may be required to return the sensitive item to the vendor.
- 3) Return the sensitive item following the vendor's instructions.
- 4) Provide "return" documentation to the person making invoice payments so that individual does not pay the invoice.

f. Unacceptable Acceptance Testing

- 1) Notify the vendor immediately that the sensitive item did not pass acceptance testing.
- 2) Make necessary arrangements with the vendor to resolve the problems or to return the unacceptable sensitive item. Authorization may be required to return the sensitive item to the vendor.
- 3) Return the sensitive item following the vendor's instructions, if applicable.
- 4) Provide "return" documentation to the person making invoice payments so that individual does not pay the invoice.

3. Marking Sensitive Items Upon Delivery

- a. To protect the agency's investment, sensitive items should be marked with a "Property of the State of Minnesota" or numbered asset label as soon as they are received and found acceptable. Numbered and unnumbered property labels can be purchased from MINNCOR Industries. A supply should be kept on hand by the person responsible for sensitive items at the agency. Engraving can also be done identifying that the property belongs to the State of Minnesota. Numbered asset labels can be used to tag sensitive items to facilitate tracking. It is recommended to use numbered asset labels for PCs.
- b. Whenever possible, sensitive items should be marked in a place clearly visible from a position in front of the sensitive item. This will facilitate identification of a sensitive item during a physical inventory or an inventory spot check. Establishing an agency standard for sensitive item label location for like sensitive items will assist the inventory coordinator/coordinator when the sensitive item label is not clearly visible.
- c. Alternate methods of marking sensitive items, such as permanent engraving, stenciling, or painting, should be considered when use of a label is inappropriate or not feasible.
- d. There are also situations in which it is not feasible to affix a label or use an alternate method to mark the sensitive item. A separate file should be maintained for these sensitive items. The file must contain a complete description of the sensitive item, and the location of the sensitive item.

- e. All ownership identification must be removed when a sensitive item is no longer owned by the state.

4. Reporting Requirements

- a. Agencies may use SWIFT or an alternative recordkeeping system to track sensitive items.

5. Agency Location Information

- a. Agency location should be reported for each sensitive item in the recordkeeping system.
- b. A location code schematic might be designed for any agency that occupies more than a few rooms. A floor plan of the agency is a useful tool in planning this design. This schematic can be as simple or elaborate as required by the agency. To be effective, a location code schematic should permit easy location of any sensitive item.

6. Disposal of State Surplus Property

- a. When it has been determined that state property is surplus to one location or division within the agency, the inventory coordinator/sub-coordinator should try to find potential users at other locations or divisions within the agency. See Intra-Agency Transfer of Sensitive items on page 5-5.
- b. If there are no potential users within the agency, the inventory coordinator/sub-coordinator should try to find potential users in other state agencies or contact Surplus Services. See Inter-Agency Transfer of Sensitive items on page 5-5.
- c. If the agency can no longer use the sensitive item and no other potential users within the state have been identified, the inventory coordinator/sub-coordinator should complete a [*Property Disposition Request*](#) form and submit it to Surplus Services.
- d. Surplus Services will assign a control number and sign the form and return a copy to the agency. Surplus Services may either approve the agency's recommended disposition of the property or authorize an alternate method of disposal. Methods of disposal include transfer to another state agency, transfer or sale to another unit of government or eligible non-profit organization, sale by sealed bid, sale by auction, negotiated sale, or scrap.
- e. The inventory coordinator/sub-coordinator is responsible for removing all State of Minnesota ownership identification from the sensitive item that is no longer owned by the state and ensuring that the sensitive item disposition is reported in the sensitive item recordkeeping system.
- f. All computers declared surplus must have data removed from their hard drives in accordance with MN.IT's Office of Enterprise Technology, Enterprise Security Information Sanitization and Destruction Standard - http://mn.gov/oet/images/SEC_S_Information_Sanitization_and_Destruction.pdf.

7. Intra-Agency Transfer of Sensitive Items

- a. Agencies must complete the Intra-Agency Transfer form (See section 10) or a similar internal inter-agency transfer document for reporting movement of sensitive items within the agency. This documentation must be maintained by the agency.
- b. The procedures in MN.IT's Office of Enterprise Technology, Enterprise Security Information Sanitization and Destruction Standard - http://mn.gov/oet/images/SEC_S_Information_Sanitization_and_Destruction.pdf must be followed, if appropriate, when items contain private or non-public data.
- c. Location information in the sensitive item recordkeeping system should be updated as the movement or transfer of sensitive items is reported.

- d. It is not necessary to submit a [*Property Disposition Request*](#) form when transferring sensitive items between divisions within the agency.

8. Inter-Agency Transfer of Sensitive Items (Movement of Sensitive Items Between State Agencies)

- a. The procedures in MN.IT's Office of Enterprise Technology, Enterprise Security Information Sanitization and Destruction Standard http://mn.gov/oet/images/SEC_S_Information_Sanitization_and_Destruction.pdf must be followed when items contain private or non-public data.
- b. To transfer surplus sensitive items to another state agency, prepare a [*Property Disposition Request*](#) form, and submit it to Surplus Services for review and approval. A copy of the form with an approval number and signature will be returned to the agency if the transfer is approved. If the transfer is not approved, the form will be returned to the agency with authorization and instructions for disposal of the surplus property.
- c. The inventory coordinator/sub-coordinator is responsible for ensuring that the sensitive item disposition is reported in the sensitive recordkeeping system.

9. Utilization of Federally-Funded Sensitive Items

- a. Additional requirements may be required for federally-funded sensitive items. State agencies must be in compliance with all state and federal requirements.
- b. Disposal of federally-owned sensitive items or sensitive items purchased with federal funds must follow any applicable federal procedures. If there are no defined federal procedures, the state procedures must be followed.

III. Sensitive Item Inventory

A. Definition of a Physical Inventory

A "physical inventory" is physically counting sensitive items. The State of Minnesota goes beyond this basic definition. In the State of Minnesota, physical inventory is the act of accounting for, and the accurate verification of, information on file for each piece of state-owned sensitive item property. In this accounting and verification process, emphasis is placed on the following aspects pertaining to each item:

1. Physically locating the sensitive items maintained on the sensitive item recordkeeping system, for the specific agency or activity.
2. Verifying that the location information on file for the sensitive item is accurate.
3. Verifying that the sensitive items are properly labeled as state property.
4. Verifying that each sensitive item in existence is reported in the sensitive item recordkeeping system.
5. Verifying that the sensitive item description is accurate.
6. Verifying that the sensitive item is in good condition for use. If the sensitive item is not in good condition, identify if it needs repairs or additional maintenance (e.g., cleaning) and report this to the appropriate personnel for action.
7. Verifying that the sensitive item is being used. If the sensitive item is not being used, determine whether it is surplus to the agency's needs or obsolete and dispose of appropriately.

B. Physical Inventory Mandated Biennially For Sensitive Items

A complete physical inventory (e.g., a wall-to-wall inventory count) for sensitive items must be conducted, at a minimum, biennially.

C. Other Conditions that may require a Physical Inventory

If one of the following conditions occurs, a physical inventory should be completed.

1. Failure of a sensitive item inventory audit. If an audit is conducted within the agency or by an outside agency, and a minimum inventory accuracy level of 95 percent is not achieved.
2. If a physical inventory was conducted and a specific area's accuracy level was below 95 percent, a physical inventory of that area should occur every six months until the acceptable 95 percent accuracy level is achieved.
3. A physical inventory should be taken whenever the person acting as inventory coordinator/ sub-coordinator is changed. The new individual in that position should conduct a physical inventory to verify the accuracy of the inventory information provided by the departing inventory coordinator/sub-coordinator. The new inventory coordinator/sub-coordinator can correct discrepancies immediately and start from a base that is accurate.

D. Planning and Scheduling the Physical Inventory

1. Plan how the physical inventory will be performed. The inventory can be performed by building, areas within the building, and activities within an agency.
2. Decide who will perform the physical inventory. The physical inventory should be performed by properly trained teams made up of agency personnel. To ensure an adequate separation of duties for internal control purposes, it is essential that the persons taking the physical inventory counts are not the same individuals responsible for reporting activity (e.g., acquisitions and dispositions) in the sensitive items recordkeeping system, unless others are involved.
3. Determine when the physical inventory should be conducted. Consideration should be given to whether personnel will be on site to open locked desks and cabinets.
4. Prepare a realistic schedule for the physical inventory, including a start date, date the initial search is expected to be completed, start date of the verification process, completion date of the verification process, and physical inventory completion date.
5. Prepare a memo explaining the physical inventory process and soliciting cooperation. Send this memo to all impacted agency personnel.
6. Obtain all supplies necessary for the physical inventory and begin the process. Necessary supplies include paper, pens, asset property labels (numbered and unnumbered), a current agency location scheme, and a current master listing of sensitive items by location. A small hand mirror is a helpful tool to see that the appropriate property label is attached to the sensitive item.

E. Conducting and Reconciling the Physical Inventory

1. Conduct the inventory in two ways. Count (1) record to sensitive item and (2) sensitive item to record.
2. When conducting a complete physical inventory, it is most effective to enter an area with a blank form (or agency designed report form) and write down the information for each sensitive item. This procedure, as opposed to entering the area with a list of sensitive items to be located, will help ensure that all sensitive items in the area are accounted for. The information recorded should include, but is

not limited to, the asset number (if one was assigned), tag number, description, location, profile id, and condition. When appropriate, the serial number and model number should be included.

3. Next, the information collected is compared to the sensitive item master listing. When an agency has multiple locations, it is preferable to sort this list in location order.
4. When discrepancies are found, they should be resolved immediately. It may be necessary to return to the location and conduct a complete search for the missing sensitive items. It may be necessary to interview employees in the area to determine the disposition of missing sensitive items. The original purchase orders for the missing sensitive items may provide helpful information to pursue in order to locate the sensitive item. If the sensitive item cannot be found, see Section IV, Stolen, Lost, Damaged, or Recovered Sensitive Items.
5. All discrepancies must be corrected in the sensitive item recordkeeping system.
6. If during the complete physical inventory, you see that the sensitive item is not being used, bring this to the attention of the inventory coordinator/sub-coordinator, who will determine whether the sensitive item is surplus to the agency's needs or obsolete and dispose of appropriately.
7. If during the complete physical inventory, you see that a sensitive item needs to be repaired, bring this to the attention of the inventory coordinator/sub-coordinator who can take the appropriate action to repair the sensitive item or follow procedures for disposal.
8. An alternative to the complete physical inventory is to conduct cycle counts of the sensitive item inventory. For example, to conduct a complete physical inventory in one year, the agency can be divided into 12 roughly equal areas. A complete physical inventory can be conducted and reconciled in a different area each month. After 12 months, the entire agency will have been inventoried. If the agency experiences many movements of sensitive items, this method may require time-consuming reconciliations each month.

F. Sensitive Item Spot Checks

1. Spot checks are an effective tool for maintaining inventory accuracy. If a specific area of the agency has consistently demonstrated a high level of inventory accuracy, one spot check between physical inventories will help keep the accuracy level high. If an area of the agency had a poor inventory accuracy level resulting from a physical inventory, spot checks should be conducted frequently in the interim until a complete physical inventory of the area has established a satisfactory accuracy level. Large agencies may wish to check a specific number of buildings or floors each month. The areas checked should be scheduled randomly.
2. When selecting sensitive items to be sampled for specific locations within the agency, the following sample size chart may be utilized.

SPOT CHECK CHART

<u>Sensitive Items in the Area</u>	<u>Minimum Sample Size</u>
1-20	All
21-50	10
51-100	15
101-200	20
201-500	25
501 or more	50

3. When spot checking the entire agency, the following sample size chart may be utilized:

SENSITIVE ITEM SPOT CHECK SAMPLE SIZE

<u>Number of Sensitive Items</u>	<u>Minimum Sample Size</u>
1-79	15
80-200	20

201-300	25
301-400	30
401-600	35
601-800	40
801-1000	45
1001-2000	50
2001-4000	75
4001 or more	100

4. To determine which sensitive items will be in the sample for the spot check, divide the total number of sensitive items by the sample size. For example, 800 total sensitive items divided by sample size of 40 equals 20, every twentieth sensitive item will be selected. To choose where to start selecting sensitive items for the spot check from the sensitive item recordkeeping system, randomly select one sensitive item out of the first 20 listed in the system. This is the first sensitive item for the spot check. The remaining sensitive items for the spot checks are every 20th sensitive item thereafter. An alternative to this approach is to select the sensitive items for the spot check using a random number table or use the internet to generate a random number sequence (e.g., <http://www.random.org>).
5. Preparations for a spot check should be similar to the planning and scheduling for the complete physical inventory.
6. The spot check procedure should be similar to conducting and reconciling the physical inventory.
7. If a sensitive item cannot be located in a reasonable length of time, it is considered “not found” for reporting purposes.
8. After the spot check procedure has been completed, a report should be prepared giving the accuracy level and discrepancies discovered in the area. Discrepancies include sensitive items that were “not found”, unmarked sensitive items, illegible asset numbers (if one was assigned), incorrect locations, and incorrect profile ids. An accuracy level of 95 percent and above is considered acceptable. Areas that fall below 95 percent accuracy should have a complete physical inventory scheduled.
9. All sensitive items found with illegible numbers (if an asset number was assigned) must be properly marked as state property.
10. All discrepancies must be corrected immediately on the recordkeeping system. Refer to the Stolen, Lost, Damaged, or Recovered Sensitive Items section below for procedures to follow when sensitive items are “not found”.

IV. Stolen, Lost, Damaged or Recovered Sensitive Items

- A. A [Stolen, Lost, Damaged or Recovered Property Report](#) must be completed under the following circumstances regardless of whether the sensitive item was located at the work site or off-site (e.g., employee has authorization to use the sensitive item at the employee’s residence):
 1. Sensitive item is stolen.
 2. Sensitive item is lost.
 3. Stolen sensitive item is recovered.
 4. Lost sensitive item is found.
- B. If the lost or stolen sensitive item contains private or non-public data, notify the agency’s data practices compliance official immediately.
- C. Immediate action should be taken to locate the sensitive item if lost or stolen.
- D. If these actions fail to locate the sensitive item within a reasonable time frame, but no longer than five business days, the loss, theft or suspected theft within the Capitol Complex area must be reported to the Department of Public Safety’s Capitol Complex Security Division. A theft or suspected theft

outside the Capitol Complex area should be report to local law enforcement authorities. Inventory coordinators/sub-coordinators should follow up with these authorities to ensure action has been taken to recover the sensitive item.

- E. A copy of the [*Stolen, Lost, Damaged or Recovered Property Report*](#) must be submitted to the agency's inventory coordinator/sub-coordinator.
- F. Notify the agency's claim officer and/or the Department of Administration's Risk Management Division claims manager of any lost, stolen, damaged, or recovered sensitive items. The claims manager will check agency sensitive item coverage. If the agency has no insurance coverage or the deductible is higher than the value of the sensitive item, then the agency must absorb the loss from its operating budget if it chooses to replace the sensitive item.
- G. A sensitive item is considered stolen if an employee fails to return a sensitive item to the state within a reasonable time frame, generally 5 business days, following the request of management for the sensitive item or upon the employee's separation from state service. The employee's manager/supervisor must take appropriate action for stolen sensitive items as noted above. The employee's manager/supervisor must also report the incident immediately to the agency Human Resources Division Director for possible disciplinary action, for recording in the employee's personnel file, and for possible reduction of employee's final pay.
- H. After an extensive search has failed to result in the recovery of the stolen or lost sensitive item, within 30 days submit a copy of the [*Stolen, Lost, Damaged or Recovered Property Report*](#) to the agency's Human Resources Division Director, Surplus Services and the Legislative Auditor's Office ([Minnesota Statutes 609.456, subd. 2](#) requires reporting in writing thefts or unlawful use of property to the Legislative Auditor).
- I. If a sensitive item is recovered, complete and submit the [*Stolen, Lost, Damaged or Recovered Property Report*](#) to the agency's Human Resources Division Director, Surplus Services and the Legislative Auditor's Office. Agencies should notify Capitol Complex Security or local law enforcement authorities that the property has been recovered. In addition, determine whether the capital asset was covered by insurance. If so, contact Admin Risk Management to determine proper disposition of the property. If the capital asset was not covered by insurance and is still usable, record the information in the agency capital asset in the recordkeeping system. If the recovered property is not usable, follow the procedures for disposal of state surplus property.
- J. Damaged, lost, or stolen sensitive items that are not recovered must be recorded in the recordkeeping system.

V. Misuse of Sensitive Items

- A. Employee misuse of a sensitive item may be subject to disciplinary action, up to and including termination.
- B. Examples of misuse of a sensitive item include, but are not limited to, the following actions:
 - 1. theft,
 - 2. damage with willful intent,
 - 3. destruction with willful intent,
 - 4. use of the sensitive item for personal gain,
 - 5. permitting other individuals to use the sensitive item for non-state purposes,
 - 6. non-return of a sensitive item when requested,
 - 7. permitting an outside consultant to use the sensitive item without a contract term allowing them to use the sensitive item, or
 - 8. inappropriate use. Employee access to and use of electronic tools is intended for business-related purposes. Limited and reasonable incidental use of these tools for occasional employee personal purpose that does not result in any additional costs or loss of time or resources for their intended business purpose is permitted. Incidental use is defined as minimal duration in length and

frequency. See [Statewide Policy: Appropriate Use of Electronic Communication and Technology](#)

- C. When misuse of a sensitive item is suspected, it should be reported immediately to the agency inventory coordinator/sub-coordinator, the Human Resources Division Director, and the appropriate manager/supervisor.

VI. Sensitive Items Used Outside the Workplace

- A. A signed agreement or inventory tracking system must be in place for state-owned sensitive items used outside of the agency-defined workplace. Employees that have a need to take a state-owned sensitive item out of the workplace should have a signed agreement. This agreement must address the conditions for their possession of the sensitive item, acceptable uses, and a requirement to return it when no longer needed for work-related use, when they depart from the division, or when requested by management. The employee's manager/supervisor must review and approve this agreement. Signed agreements must be kept on file. If there is no signed agreement, the agency must ensure that the employee is informed of the appropriate use of the sensitive item and the requirement to return it when no longer needed for work-related use. A sample agreement is provided in the Forms Section (Section 10).
- B. Agencies allowing individuals to take state-owned property which contains private or non-public data outside the workplace must ensure that appropriate procedures are in place to prevent unauthorized access to the private or non-public data.
- C. An employee's use of state property outside the workplace should be consistent with the [statewide telecommuting policy](#) and the employee's agency telecommuting policy.
- D. The agency's sensitive item recordkeeping system must include data indicating what sensitive items are used outside the workplace and by whom (employee name, or consultant name and contract number).
- E. Certain statutes address state employee use of state property. [Minnesota Statutes 16B.55](#) specifies permitted and prohibited uses of state vehicles. Also, [Minnesota Statutes 43A.38](#) states that inappropriate use of state property is a violation of the Code of Ethics for Employees in the Executive Branch.
- F. Examples of inappropriate use of sensitive items outside the workplace include, but are not limited to the following:
 - 1. using the sensitive item for personal use without express statutory authority (e.g., using a computer for a personal business),
 - 2. giving the sensitive item to the employee as a gift or transferring ownership of the sensitive item to the employee outside of public sale, or
 - 3. permitting non-state employee use, including consultants without contractual provisions which allow off-site use of sensitive items.
- H. Contractors may be permitted to use sensitive items off-site provided their agreement with the state identifies the sensitive items, requires that the sensitive items are returned to the state upon termination of the contract or by request if allowed by contract terms, and states that inappropriate use of such sensitive items is prohibited.