

State of Vermont
Department of Finance and Management

Business Process:	Employee Separation	Issue Date:	August 2007
		Number:	BP-08
Topic:	Internal Control - Best Practices	Revision Date:	N/A
Applicable To:	All State Agencies, Departments, and Offices	Page:	1 of 3

Objective

When employees separate or transfer to another position within State service, departments are responsible for ensuring that the State's assets are protected and that any department owned property has been returned.

Risks

- Unauthorized access and use of assets (e.g. equipment, facilities, IT systems, credit cards, data, etc.)
- Lost, stolen, or damaged assets
- Unsecured work environment for personnel

Definition

Separate: When an employee leaves state service for reasons including, but not limited to, resignations, retirements, reductions-in-force, death, and dismissals.

Best Practices Include

[Refers to category of [Control Activity](#) as described in [Internal Control Standards: A Guide for Managers](#)]

- ❖ Utilize a **checklist** to ensure a consistent, thorough, and documented procedure. [Documentation]
- ❖ Tailor the components of the checklist to reflect each department's operating environment (*even within a department, not all items on the checklist will be applicable to all employees*). [Safeguarding of Assets]
- ❖ Depending on the contents, it may be necessary to assign different staff to complete individual sections of the checklist, but one staff person (e.g. personnel officer, business manager, employee's supervisor) should be delegated overall responsibility for ensuring the checklist is completed. [Authorization]

Financial Process:	Employee Separation	Issue Date:	August 2007
		Number:	BP-08
Topic:	Internal Control - Best Practices	Revision Date:	N/A
Applicable To:	All State Agencies, Departments, And Offices	Page:	2 of 3

- ❖ When department property is returned, the recovered items should be indicated on the checklist and signed by the separating employee and staff person who took custody of the items.

[\[Verification and Safeguarding of Assets\]](#)

- ❖ Complete the separation checklist, including any necessary remedial actions, prior to the employee's last working day (*when possible*) to allow time for resolving outstanding issues before termination.

[\[Safeguarding of Assets\]](#)

- ❖ Inform executive management (e.g. secretary, commissioner, or their deputies, etc.) when a separating employee does not return department property and take appropriate actions to resolve.

[\[Compliance\]](#)

- ❖ The checklist should be reviewed and approved by the staff person who has been delegated responsibility for completion; exceptions should be investigated and actions taken should be noted.

[\[Approval\]](#)

- ❖ Separation checklists should be retained as official department records.

[\[Documentation\]](#)

- Following are some items a department should consider for its employee separation checklist. This list is not intended to be all-inclusive and, as previously stated, not every item will be applicable to every employee, nor to every department.

- Keys (building, office, desk, file cabinets, safes, equipment, vehicle, etc)
- Security/ID Badge
- State Credit Cards including Purchasing Card
- Parking Permit
- Final Employee Timesheet and Expense Account Submitted
- Outstanding Travel or Salary Advances
- Exit Interview and Performance Evaluation
- Computer Equipment (e.g. Laptops, Portable Printers, etc)
- Handheld Devices (e.g. BlackBerry, Palm Pilot, portable storage devices, etc)
- Pagers
- Cellular Phones

Financial Process:	Employee Separation	Issue Date:	August 2007
		Number:	BP-08
Topic:	Internal Control - Best Practices	Revision Date:	N/A
Applicable To:	All State Agencies, Departments, And Offices	Page:	3 of 3

- Uniforms
- Vehicles
- Other Equipment (e.g. tools, firearms, etc)
- Proprietary and/or Confidential Documents
- Disable Network Access
- Disable E-mail Account
- Revoke Access to IT Systems (e.g. VISION, HCM, Department Systems, Federal Systems, etc)
- Change System Administrator Password(s)
- Change Common Passwords (e.g. non-employee specific used for ordering from suppliers or vendors)
- Change Keypad/Combination Locks
- Disable Long-Distance Calling Access Number
- Change Voice-Mail
- Cancel any Services/Subscriptions/Memberships Paid by the Department for the Employee
- Remove Employee Name from Department Documents (e.g. website, contacts list, signature authorizations, bank accounts, etc)
- Notification to Customers, Vendors, Clients, etc.

Notices

- These best practices are intended to support the internal control framework as presented in the [**Internal Control Standards: A Guide for Managers.**](#)
- In consideration of these best practices, the objective should be on adherence and not on rationalizing ways and means for circumvention.
- Nothing in this document shall limit or supersede any applicable Federal or State laws, statutes, bulletins, or regulations.