**Use Cases and Non-Use Cases for the Inventory System**

**1. Use Cases**

**Use Case 1: Add a New Asset (Component)**

**Actor:** Admin/Staff  
**Preconditions:** Employee is authenticated.  
**Main Scenario:**

1. User selects asset type (e.g., GPU, keyboard).
2. User fills in fields (ID, name, condition, cost, status, location, etc. per asset type).
3. System validates fields and uniqueness of ID.
4. Asset is inserted into correct table.
5. Confirmation displayed.

**Alternative Scenarios:**

* Required fields missing → error, highlight missing fields.
* Duplicate ID → error, user must correct.

**Use Case 2: Edit an Existing Asset**

**Actor:** Admin/Staff  
**Preconditions:** Asset exists, employee is authenticated.  
**Main Scenario:**

1. User locates asset via search or list.
2. User edits fields (status, location, etc.).
3. System validates and updates the record.
4. Confirmation displayed.

**Alternative:**

* User tries to change ID or link to non-existent component (in PC setup) → error shown.

**Use Case 3: Create/Edit/Delete PC Setup**

**Actor:** Admin/Staff  
**Preconditions:** All components to be linked exist.  
**Main Scenario:**

1. User starts new/edit PC setup.
2. User selects component IDs for each field.
3. System validates all references exist.
4. Setup is created/updated/deleted.
5. Confirmation shown.

**Alternative:**

* One or more referenced IDs do not exist → error.

**Use Case 4: View and Export Reports**

**Actor:** Admin/Staff  
**Main Scenario:**

1. User selects a report (totals, disposed, stored).
2. System queries the relevant view.
3. Report shown in UI.
4. User can export as CSV.

**Alternative:**

* No data in report → "No records found" message.

**Use Case 5: Manage Employees**

**Actor:** Admin/Admin (DBA)  
**Main Scenario:**

1. Admin adds/edits/deletes employee records.
2. System enforces unique email and required fields.
3. Password is hashed on creation/update.
4. Confirmation displayed.

**Alternative:**

* Attempt to add with existing email → error.

**Use Case 6: Employee Authentication**

**Actor:** Employee  
**Main Scenario:**

1. Employee enters ID/email and password.
2. System hashes and checks credentials.
3. On success, employee is logged in; otherwise, error.

**2. Non-Use Cases**

* Rental or reservation of assets.
* Financial tracking or transactions.
* Automated notifications.
* Advanced analytics/dashboarding beyond reporting views.
* External system integration.
* Self-service for non-employee users.