**Use Case:** Add Resource

**Actor:** Manager

**Preconditions:** A User has a authentication Token. The Authorization Server is running. The database is running.

**Postconditions:** A new resource has been added to the database. A response has been sent to the user.

**Scenario:**

* 1. A POST HTTPS request is received by the system
  2. The system extracts the authentication token from the request
  3. The system creates a REST API request to send to the Authentication Server with the token
  4. The system sends the HTTPS request to the Authentication server
  5. The Authentication server sends back a response
  6. The system verifies that the data it receives is of a valid format
  7. The system gets the user title from the Authentication server response
  8. The system verifies the resource is valid
  9. The system creates a SQL statement to add the new resource to the database
  10. The system sends the request to the database
  11. The system receives the database response and packages to send back to the user as JSON
  12. The system sends back a HTTPS response to the user

**Special Requirements: fill**

**Technology and Data Variations List: fill**

**Use Case:** Query Resource Types

**Actor:** Manager, Employee

**Preconditions:** A User has a authentication Token. The Authorization Server is running. The database is running.

**Postconditions:** The resource types have been returned to the user.

**Scenario:**

* 1. A HTTPS GET request is received by the system
  2. The system extracts the authentication token from the request
  3. The system creates a REST API request to send to the Authentication Server with the token
  4. The system sends the HTTPS request to the Authentication server
  5. The Authentication server sends back a response
  6. The system verifies that the data it receives is of a valid format
  7. The system gets the user title from the Authentication server response
  8. The system verifies the resource is valid
  9. The system creates a SQL statement to query the resource types
  10. The system sends the request to the database
  11. The system receives the database response and packages it to send back to the user as JSON
  12. The system sends back a HTTPS response to the user

**Special Requirements:** fill

**Technology and Data Variations List:** fill

**Use Case:** Query Resources

**Actor:** Manager, Employee

**Preconditions:** A User has a authentication Token. The Authorization Server is running. The database is running.

**Postconditions:** The resources in the database have been returned to the user.

**Scenario:**

* 1. A HTTPS GET request is received by the system
  2. The system extracts the authentication token from the request
  3. The system creates a REST API request to send to the Authentication Server with the token
  4. The system sends the HTTPS request to the Authentication server
  5. The Authentication server sends back a response
  6. The system verifies that the data it receives is of a valid format
  7. The system gets the user title from the Authentication server response
  8. The system verifies the resource is valid
  9. The system creates a SQL statement to query all of the resources
  10. The system sends the request to the database
  11. The system receives the database response and packages it to send back to the user as JSON
  12. The system sends back a HTTPS response to the user

**Special Requirements:** fill

**Technology and Data Variations List:** fill

**Use Case:** Delete Resource

**Actor:** fill

**Preconditions:** A User has a authentication Token. The Authorization Server is running. The database is running.

**Postconditions:** The resource has been labeled deleted in the database

**Scenario:**

* 1. A HTTPS POST request is received by the system
  2. The system extracts the authentication token from the request
  3. The system creates a REST API request to send to the Authentication Server with the token
  4. The system sends the HTTPS request to the Authentication server
  5. The Authentication server sends back a response
  6. The system verifies that the data it receives is of a valid format
  7. The system gets the user title from the Authentication server response
  8. The system verifies the resource is valid
  9. The system creates a SQL statement to delete the specified resource
  10. The system sends the request to the database
  11. The system receives the database response and packages it to send back to the user as JSON
  12. The system sends back a HTTPS response to the user

**Special Requirements:** fill

**Technology and Data Variations List:** fill

**Use Case:** Modify Resource

**Actor:** Manager

**Preconditions:** A User has a authentication Token. The Authorization Server is running. The database is running.

**Postconditions:** The resource has been modified in the database. A response has been sent to the user

**Scenario:**

* 1. A HTTPS PUT request is received by the system
  2. The system extracts the authentication token from the request
  3. The system creates a REST API request to send to the Authentication Server with the token
  4. The system sends the HTTPS request to the Authentication server
  5. The Authentication server sends back a response
  6. The system verifies that the data it receives is of a valid format
  7. The system gets the user title from the Authentication server response
  8. The system verifies the resource is valid
  9. The system creates a SQL statement to modify the specified resource
  10. The system sends the request to the database
  11. The system receives the database response and packages it to send back to the user as JSON
  12. The system sends back a HTTPS response to the user

**Special Requirements:** fill

**Technology and Data Variations List:** fill