|  |  |
| --- | --- |
| UC Name | UC\_9: Bank Employee Views Client Accounts |
| Summary | This use case allows a bank employee to view all client accounts. The employee must be authorized to access account details, and the system ensures secure retrieval and display of information.. |
| Dependency | This use case depends on the authentication and authorization system to verify the employee's credentials. |
| Actors | * **Primary Actor:** Bank Employee * **Secondary Actor:** Banking System |
| Preconditions | 1. The bank employee must be logged into the banking system. 2. The employee must have the necessary permissions to access client accounts. 3. The banking system must be online and operational. |
| Description of the main sequence | 1.The bank employee logs into the system.  2.The employee selects the option to view client accounts.  3.The employee asks for permission from the client to access his/her rights.  4.The system verifies the employee’s access rights.  5.The system retrieves and displays a list of all client accounts.  6.The employee can select a specific client account to view details.  7.The system displays the detailed information of the selected client account. |
| Description of the alternative sequence | 1. If the employee is not logged in, they are prompted to log in. 2. If the employee does not have sufficient permissions, an error message is displayed. 3. If the system is offline, an appropriate error message is shown.. |
| Non functional requirements | * **Performance:** The system should retrieve and display client accounts within 2 seconds. * **Security:** Only authorized employees should access client account details. * **Availability:** The system should be accessible 99.9% of the time. |
| Postconditions | * The bank employee successfully views the client accounts. * The system logs the employee’s access for auditing purposes. * No unauthorized data modifications occur during the process. |

A flowchart with text and images

AI-generated content may be incorrect.

|  |  |
| --- | --- |
| UC Name | UC\_10 Update Client Account Information |
| Summary | This use case allows a bank employee to update client account information. The employee must be authorized to modify account details, ensuring secure and accurate updates. |
| Dependency | This use case depends on the authentication and authorization system to verify the employee's credentials. It may also depend on the "View Client Accounts" use case to retrieve account details before updates.. |
| Actors | * **Primary Actor:** Bank Employee * **Secondary Actor:** Banking System |
| Preconditions | 1. The bank employee must be logged into the banking system. 2. The employee must have the necessary permissions to update client account information. 3. The banking system must be online and operational. 4. The client account must exist in the system. |
| Description of the main sequence | 1. The bank employee logs into the system. 2. The employee selects the option to update client account information. 3. The system verifies the employee’s access rights. 4. The system retrieves and displays the client’s current account information. 5. The employee makes the necessary changes to the account details. 6. The system validates the updated information. 7. The employee confirms the changes. 8. The system updates the client account in the database. 9. The system logs the update for audit purposes. T 10. The system notifies the employee that the update was successful |
| Description of the alternative sequence | * If the employee is not logged in, they are prompted to log in. * If the employee does not have sufficient permissions, an error message is displayed. * If the system is offline, an appropriate error message is shown. * If the account does not exist, the system displays an error message. * If the updated information is invalid, the system prompts the employee to correct it. * If the update fails due to a system error, the employee is notified, and the update is logged as unsuccessful. |
| Non functional requirements | * **Performance:** The system should process account updates within 3 seconds. * **Security:** Only authorized employees should be able to modify client account details. * **Auditability:** Every update must be logged for tracking and compliance. * **Availability:** The system should be accessible 99.9% of the time |
| Postconditions | * The client account information is successfully updated. * The system logs the update for auditing purposes. * The employee receives confirmation of the successful update. * The updated information is available for future queries and transactions |

A flowchart of information

AI-generated content may be incorrect.

|  |  |
| --- | --- |
| UC Name | UC\_11: Bank Employee Checks Client Loan Status. |
| Summary | This use case allows a bank employee to check the loan status of a client. The employee must have appropriate authorization to access the loan details, ensuring secure and accurate retrieval of information.. |
| Dependency | |  | | --- | |  |   This use case depends on the authentication and authorization system to verify the employee's credentials. It may also depend on the "View Client Accounts" use case to retrieve client details before accessing the loan status |
| Actors | * **Primary Actor:** Bank Employee * **Secondary Actor:** Banking System |
| Preconditions | |  | | --- | | 1. The bank employee must be logged into the banking system. 2. The employee must have the necessary permissions to access client loan details. 3. The banking system must be online and operational. 4. The client must have an active loan account in the system. | |
| Description of the main sequence | 1. The bank employee logs into the system. 2. The employee selects the option to check client loan status. 3. The system verifies the employee’s access rights. 4. The employee enters or selects the client’s account. 5. The system retrieves and displays the loan status, including outstanding balance, due dates, and payment history. 6. The employee reviews the loan details. 7. The system logs the access request for audit purposes.. |
| Description of the alternative sequence | 1. If the employee is not logged in, they are prompted to log in. 2. If the employee does not have sufficient permissions, an error message is displayed. 3. If the system is offline, an appropriate error message is shown. 4. If the client does not have a loan, the system displays a message stating no active loans. 5. If the loan details cannot be retrieved due to a system error, the employee is notified, and the access attempt is logged as unsuccessful.. |
| Non functional requirements | * **Performance:** The system should retrieve and display loan details within 3 seconds. * **Security:** Only authorized employees should be able to access client loan details. * **Auditability:** Every loan status check must be logged for tracking and compliance. * **Availability:** The system should be accessible 99.9% of the time. |
| Postconditions | * The employee successfully retrieves and views the client’s loan status. * The system logs the access request for auditing purposes. * No unauthorized modifications are made to the loan data. * The retrieved information is available for further processing or customer inquiries. |

A flowchart of a bank

AI-generated content may be incorrect.

|  |  |
| --- | --- |
| UC Name | UC\_12: Administrator Manages Employee Accounts. |
| Summary | This use case allows an administrator to manage employee accounts, including creating, updating, deactivating, and viewing employee information. The administrator must have the necessary permissions to perform these actions securely and efficiently. |
| Dependency | |  | | --- | |  |   This use case depends on the authentication and authorization system to verify the administrator's credentials. It may also depend on the "Employee Authentication" use case for login and access control |
| Actors | * **Primary Actor:** Administrator * **Secondary Actor:** Banking System |
| Preconditions | |  | | --- | | 1. The administrator must be logged into the banking system. 2. The administrator must have the required permissions to manage employee accounts. 3. The banking system must be online and operational. | |
| Description of the main sequence | 1. The administrator logs into the system. 2. The administrator selects the option to manage employee accounts. 3. The system verifies the administrator’s access rights. 4. The administrator can perform the following actions:    * Create a new employee account by entering relevant details.    * Update an existing employee's information.    * Deactivate an employee account if necessary.    * View employee account details. 5. The system validates and saves the changes. 6. The system logs the changes for audit purposes. 7. The system notifies the administrator that the action was successful.  |  |  | | --- | --- | |  |  | |
| Description of the alternative sequence | 1. -If the administrator is not logged in, they are prompted to log in. 2. If the administrator does not have sufficient permissions, an error message is displayed. 3. If the system is offline, an appropriate error message is shown. 4. If the entered employee information is invalid, the system prompts the administrator to correct it 5. If an update or deactivation fails due to a system error, the administrator is notified, and the attempt is logged as unsuccessful |
| Non functional requirements | * **Performance:** The system should process employee account actions within 3 seconds. * **Security:** Only authorized administrators should be able to manage employee accounts. * **Auditability:** Every account management action must be logged for tracking and compliance.   **Availability:** The system should be accessible 99.9% of the time. |
| Postconditions | * The administrator successfully performs the requested account management action. * The system logs all changes for auditing purposes. * No unauthorized modifications occur. * The updated employee account information is available for future access and verification. |

A diagram of a company

AI-generated content may be incorrect.