|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC01 | |
| Use Case Name | User Authentication | |
| Scenario | User wants to Log in to the system | |
| Triggering Event | Log In | |
| Brief Description | When the admin access his files authentication is required. | |
| Actor(s) | Administrator | |
| Related Use Cases | ---- | |
| Stakeholders | Administrator, Client | |
| Precondition | User must plugin the Flash drive to the PC | |
| Post Condition | Administrator must able to access the system | |
| Basic Flow: | Actor’s Action | System’s Response |
|  | 1: Opens the application | 1.1: System displays the login page of the application |
| 2: User types its username/password |  |
| 3: User clicks login button | 3.1: System checks the database if the username and password is correct |
|  | 3.2: username and password matched System will message (SM01) |
|  | 3.3: System appears the main page of the application |
|  | 3.4: System scans for corrupted text file |
|  |  |  |
| Alternative Flow: |  | 3.2: If username and password of Administrator didn’t match |
|  |  | 3.3: System displays message (SM02) |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC02 | |
| Use Case Name | User back-ups text files | |
| Scenario | User request for back-up | |
| Triggering Event | Back-up Text files | |
| Brief Description | As a prevention mechanism on data corruption, an automatic real-time backup is running on background. | |
| Actor(s): | Administrator | |
| Related Use Cases | User Authentication | |
| Stakeholders | Administrator, Client | |
| Precondition | User opens an text application | |
| Post condition | User was able to back-up the text file automatically while working on text application | |
| Basic Flow: | Actor Action | System Response |
|  | Step 1: User Plug’s in the Flash Drive | 1.1: System checks if the flash drive is less than 80% of the storage |
|  | 1.2: System scans for corrupted text file |
|  | 1.3: System will identify If the corrupted data can be fixed or not. |
|  | 1.4 Fix corrupted data |
| 2: User opens text file application | 2.1: System will start executing automatic real-time back up |
|  | 2.2: System will calculate if the storage can accumulate the back-up file. |
|  | 2.3: System backed-up text file |
|  |  |
|  |  |  |
| Alternative Flow: |  | 1.3: System will identify If the corrupted data can be fixed or not. |
|  | 2. User Agrees to delete corrupted data | 2.1 Delete Corrupted data. |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC03 | |
| Use Case Name | User views log | |
| Scenario | Admin views logs | |
| Triggering Event | View Logs | |
| Description | The changes made in the Flash drive are recorded in the logs. | |
| Actor(s) | Administrator | |
| Related Use Case | Use Authentication | |
| Stakeholders | Administrator | |
| Precondition | User is logged in as Admin | |
| Post Condition | User is able to view the in/out of text file | |
| Basic Flow: | Actor Action | System Response |
|  | 1: User view logs. | 1.1: System displays “Daily logs” and “Weekly logs” |
| 2. User select “Daily logs” | 2.1: System displays “Daily logs” page |
| 3. User select “Weekly logs” | 3.1: System displays “Weekly logs” page |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC04 | |
| Use Case Name | User retrieve text file | |
| Scenario | User wants to get the back-up text file | |
| Triggering Event | Retrieve Text File | |
| Brief Description | Admin retrieves files that we’re backed up. | |
| Actor(s) | Administrator | |
| Related Use Case | User Authentication, User Back-Up | |
| Stakeholders | Administrator, Client | |
| Precondition | User has a back-up text files | |
| Post condition | Admin was able retrieve the back-up files | |
| Basic Flow: | Actor Action | System Response |
|  | 1. Admin will Select & Copy the file to retrieve |  |
| 1. Admin will Paste the retrieved file. |  |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC08 | |
| Use Case Name | Log out | |
| Scenario | User wants to log out from the system | |
| Triggering Event | Log out | |
| Brief Description | Log out from the system | |
| Actor(s) | Administrator | |
| Related Use Case | User Authentication | |
| Stakeholders | Administrator, Client | |
| Precondition | Admin is logged in | |
| Post condition | Admin was able to log out the system | |
| Basic Flow: | Actor Action | System Response |
|  | 1. Clicks the Logout button |  |
|  | 1. Destroys the session and logs out from the system 2. Displays the Log In page |

|  |  |
| --- | --- |
| System Message | |
| SM01 | You logged in successfully! |
| SM02 | Username or password is incorrect! |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC05 | |
| Use Case Name | Scan Corrupted Text file | |
| Scenario | User wants to know if there’s any corrupted text file | |
| Triggering Event | Scan | |
| Brief Description | System scans for the corrupted text file | |
| Actor(s) | Administrator | |
| Related Use Case | User Authentication | |
| Stakeholders | Administrator, Client | |
| Precondition | Admin is logged in | |
| Post condition | Admin was able to log out the system | |
| Basic Flow: | Actor Action | System Response |
|  | 1. Log In’s the application |  |
|  | 1. Automatically scans for the corrupted text file |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC06 | |
| Use Case Name | Download Log | |
| Scenario | User wants to review logs | |
| Triggering Event | Logs | |
| Brief Description | To review the systems activity | |
| Actor(s) | Administrator | |
| Related Use Case | User Authentication, View logs | |
| Stakeholders | Administrator, Client | |
| Precondition | User must have logged in as Administrator | |
| Post condition | Admin was able to download the logs | |
| Basic Flow: | Actor Action | System Response |
|  | 1. Admin clicks “View Logs” | 1.1 Displays the View Logs page |
| 1. Admin clicks “Download Logs” | 2.1 System download logs |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC07 | |
| Use Case Name | Memory Check | |
| Scenario | User wants to know the memory space of the flash drive | |
| Triggering Event | Memory Checking | |
| Brief Description | Able to identify the available memory space of the flash drive | |
| Actor(s) | Administrator, client | |
| Related Use Case | User Authentication | |
| Stakeholders | Administrator, Client | |
| Precondition | User must have logged in | |
| Post condition | User was able to know the memory space of the flash drive | |
| Basic Flow: | Actor Action | System Response |
|  | 1. Enter credentials | 1.1 Automatically Scans for the corrupted text file |
|  | 1. Scanned Complete |
|  |  | 1. Checks the memory space |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC09 | |
| Use Case Name | User views daily logs | |
| Scenario | Admin views logs | |
| Triggering Event | View Logs | |
| Description | The changes made in the Flash drive are recorded in the logs. | |
| Actor(s) | Administrator | |
| Related Use Case | Use Authentication | |
| Stakeholders | Administrator | |
| Precondition | User is logged in as Admin  User selected view logs | |
| Post Condition | User is able to view the in/out of text file | |
| Basic Flow: | Actor Action | System Response |
|  | 1. User select “Daily logs” | 1.1: System displays “Daily logs” page |
|  |  | 1.2: System will retrieve log data |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC10 | |
| Use Case Name | User views weekly logs | |
| Scenario | Admin views logs | |
| Triggering Event | View Logs | |
| Description | The changes made in the Flash drive are recorded in the logs. | |
| Actor(s) | Administrator | |
| Related Use Case | Use Authentication | |
| Stakeholders | Administrator | |
| Precondition | User is logged in as Admin  User selected view logs | |
| Post Condition | User is able to view the in/out of text file | |
| Basic Flow: | Actor Action | System Response |
|  | 1. User select “Weekly logs” | 1.1: System displays “Weekly logs” page |
|  |  | 1.2: System will retrieve log data |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC011 | |
| Use Case Name | Repair Data | |
| Scenario | User wants to repair corrupted data | |
| Triggering Event | Repair | |
| Brief Description | When the admin wants to repair corrupted data | |
| Actor(s) | Administrator | |
| Related Use Cases | ---- | |
| Stakeholders | Administrator, Client | |
| Precondition | User must plugin the Flash drive to the PC | |
| Post Condition | Administrator must able to access the system | |
| Basic Flow: | Actor’s Action | System’s Response |
|  | 1: User must click the repair page | 1.1: System will display repair page |
| 2: User click the repair button | 2.1 System will try to repair the damage data. |
| Alternative Flow: |  |  |
|  |  | 3.3: System displays message (SM05) |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC012 | |
| Use Case Name | Register | |
| Scenario | User wants to create an account to the system | |
| Triggering Event | Register | |
| Brief Description | When the user creates an account for authentication | |
| Actor(s) | Administrator, user | |
| Related Use Cases | User Authentication | |
| Stakeholders | Administrator, Client | |
| Precondition | User must plugin the Flash drive to the PC | |
| Post Condition | Administrator must able to access the system | |
| Basic Flow: | Actor’s Action | System’s Response |
|  | 1: User connected the flash drive | 1.1: System displays the login page of the application |
| 2: User does not have a valid account |  |
| 3: User clicks register button | 3.1: Displays registration page |
|  | 3.2: Complete account creation system displays (SM01) |
|  |  |  |
| Alternative Flow: |  |  |
|  |  | 3.3: System displays message (SM02) |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC013 | |
| Use Case Name | System Start up | |
| Scenario | User wants to start the system | |
| Triggering Event | User wants to use the system | |
| Brief Description | When the admin wants to use the tool. | |
| Actor(s) | Administrator, User | |
| Related Use Cases | ---- | |
| Stakeholders | Administrator, Client | |
| Precondition | ---- | |
| Post Condition | Administrator must able to access the system | |
| Basic Flow: | Actor’s Action | System’s Response |
|  | 1: User Inserts flash drive | 1.1: Flash drive detected |
| 2: User click the Hydra Data Protection. Exe | 2.1: the “Hydra Dara Protection system will load” |
| Alternative Flow: |  |  |
|  |  | 3.2: System displays message (SM06) |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC014 | |
| Use Case Name | Home Page | |
| Scenario | User wants to see details about the system | |
| Triggering Event | Home Page | |
| Brief Description | When the admin wants to view the details of the system | |
| Actor(s) | Administrator | |
| Related Use Cases | ---- | |
| Stakeholders | Administrator, Client | |
| Precondition | User must plugin the Flash drive to the PC  User must logged in | |
| Post Condition | Administrator must able to access the system | |
| Basic Flow: | Actor’s Action | System’s Response |
|  | 1: Clicks the home page button | 1.1: System displays the Home page of the application |
| Alternative Flow: |  |  |
|  |  | 1.2: System displays message (SM07) |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC015 | |
| Use Case Name | Power outage data prevention | |
| Scenario | The system should save data even after power loss. | |
| Triggering Event | Back-up | |
| Brief Description | The admin wants to protect the data from data loss | |
| Actor(s) | Administrator | |
| Related Use Cases | ---- | |
| Stakeholders | Administrator, Client | |
| Precondition | User must plugin the Flash drive to the PC | |
| Post Condition | Administrator must able to access the system | |
| Basic Flow: | Actor’s Action | System’s Response |
|  | 1. The user must click the back-up button |  |
|  | 2 an instance of a file is backed up | * 1. System’s power cuts off |
|  |  | * 1. The file backed-up should remain at the flash drive |
| Alternative Flow: | N/A | N/A |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC016 | |
| Use Case Name | Decryption | |
| Scenario | The system should decrypt the files after log-in | |
| Triggering Event | Log-in | |
| Brief Description | The system should decrypt the data | |
| Actor(s) | System | |
| Related Use Cases | ---- | |
| Stakeholders | Administrator, Client | |
| Precondition | User must plugin the Flash drive to the PC | |
| Post Condition | Administrator must able to access the system | |
| Basic Flow: | Actor’s Action | System’s Response |
|  | 1. the user must click the log-in button | 1.1 the system will log-in to the system |
|  |  | 1.2 the system will decrypt the files on the flash drive. |
|  |  |  |
| Alternative Flow: |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Number | PICDS-UC017 | |
| Use Case Name | Encryption | |
| Scenario | The system should encrypt the files after log-out | |
| Triggering Event | Log-out | |
| Brief Description | The system should encrypt the data | |
| Actor(s) | System | |
| Related Use Cases | ---- | |
| Stakeholders | Administrator, Client | |
| Precondition | User must plugin the Flash drive to the PC | |
| Post Condition | Administrator must able to access the system | |
| Basic Flow: | Actor’s Action | System’s Response |
|  | 1. the user must click the log-out button | 1.1 the system will log-out to the system |
|  |  | 1.2 the system will encrypt the files on the flash drive. |
|  |  |  |
| Alternative Flow: |  |  |
|  |  |  |