Washington State Patrol

Criminal Records Division

Request for Proposal for

The WSP Web Portal Project
Appendix C: Functional Requirements

RFP #: WSP-RFP-WEB001
RFP Issue Date: 5/4/20

Document Control Page

Document Status: Final
Document Date: February 14, 2020

Document Purpose

This document is the WSP Web Portal – Appendix A: Functional Requirements.

Version	Date	By	Description/Changes

TABLE OF CONTENTS

Page

1 FUNCTIONAL REQUIREMENTS

1.1 Background

The Washington Access to Criminal History (WATCH) is a public facing interface that allows parties to conduct Name/Date of Birth (NDOB) background checks against the Washington State Identification System (WASIS) Criminal History Repository. This web-based application also includes interfaces designed for the Criminal Justice community, Washington State and Federal agencies. As part of the W2 Replacement Project, the Washington State Patrol (WSP) Criminal Records Division (CRD) is reexamining how they can better interact with their customers by expanding the functionality of WATCH.

This document attempts to capture all requirements regardless of whether they are already provided by WATCH or are considered a new requirement to be first implemented in the portal in order to provide a complete inventory of all currently known components for the portal. In addition, it contains requirements that are part of WASIS but pertain to the WSP Web Portal.

1.2 The WSP Web Portal

WSP is looking for a platform that will allow every WSP customer to securely communicate with the CRD. Customers using a secure ID and password, and (when applicable) two-factor authentication can log onto a secure site and read and send messages, request documents and services, and receive billing information. WSP has an extremely diverse customer base with great variation in their comfort with web-based services. Any solution must be able to serve as wide and diverse a community as possible and provide a consistent high-quality experience for all users of the web portal. Any solution must be shown to be efficient and cost effective to upgrade, maintain software currency, and have a framework that can support changes and further development.

1.2.1 Online Banking

The closest analogy for the web portal pattern WSP wants is that which is used by the online banking industry. In this pattern, bank customers create and maintain their IDs, passwords, and (where applicable) secondary authentication for pre-existing accounts. Once established customers supply contact information and elect to receive notifications. A message queue associated with their account allows customers to converse with the bank's business units. If elected, a text message is sent to a registered email address to notify the user of a change or action to their account, or the presence of a new message in their queue. Bank customers also have a transaction history where they can view documents such as monthly statements or deposit reports or locate cancelled checks. A bank customer can access online services such as balance transfer, bill payment or requesting checks. Contact management allows bank customers to update or change their name, address, and other contact information and identify their preferred methods for contact. Customers can upload critical documents to a secure location and receive notification that their document has been received. The user experience is secure, stable and consistent.

1.2.2 WSP Administered Account

The WSP Web Portal adheres to a pattern very similar to that offered by online banking services for Administered Accounts. These customers must submit paperwork to CRD and that provides the legal basis to establish their account. CRD establishes the skeletal structure of the account based on the submission

and then contacts the customer, providing the initial ID and temporary password. The customer can modify or expand contact information, manage notifications, send and receive message queues, etc. In addition, these customers may be offered subscription services such as Rapback or be granted access to reporting services to request select reports. CRD tracks the activities of these customers as either "billed" (customers they invoice for services) or "non-billed." (Entities that is not charged for services).

1.2.3 Online Retail Shopping

While the WSP Web Portal exploits the online banking pattern for their administered accounts, WSP believes that the closest analogy for the general public's access is online retail shopping pattern. In this pattern, the retail customers create and maintain their IDs, passwords, and (where applicable) secondary authentication when they create their accounts. Unlike the banking pattern that require the intervention of bank to establish the account, shoppers establish their own accounts, supply contact information and elect to receive notifications. There is a message queue associated with their account to allow customers to converse with customer support units. If elected, a text message is sent to a registered email address to notify the user of a change or action to their account, or the presence of a new message in their queue. Retail customers setup their credit card payment information and have access to a transaction history where they can view documents such as order confirmations and invoices. A retail customer can order goods or services and pre-pay with their credit card. Contact management allows retail customers to update or change their name, address, and other contact information (billing, shipping, alternate shipping addresses) and identify their preferred methods for contact. The user experience is secure, stable and consistent.

1.2.4 WSP Public Customers

Through its WATCH application WSP currently offers the general public the ability to create and maintain their own accounts where they can perform NDOB search service by pre-paying with a credit card. These public customers create and maintain their contact management. They securely communicate with WSP staff through notifications and messages, but own and maintain their accounts. Results of search requests go to their transaction history where they can be viewed, printed or downloaded.

1.3 Universal Business Processes

Universal Business Processes are those common for all actors using the portal. These requirements are generic in nature because they are applicable to more than one specific process.

1.3.1 Universal Business Process Description

These business processes apply to all customers. Requirements that are not universally applicable are listed in the business process (es) for which they are relevant.

1.3.2 Process Descriptions

The portal must be simple to administer, but provide customers with a single point of entry where they can: perform tasks, retrieve documents and communicate with CRD.

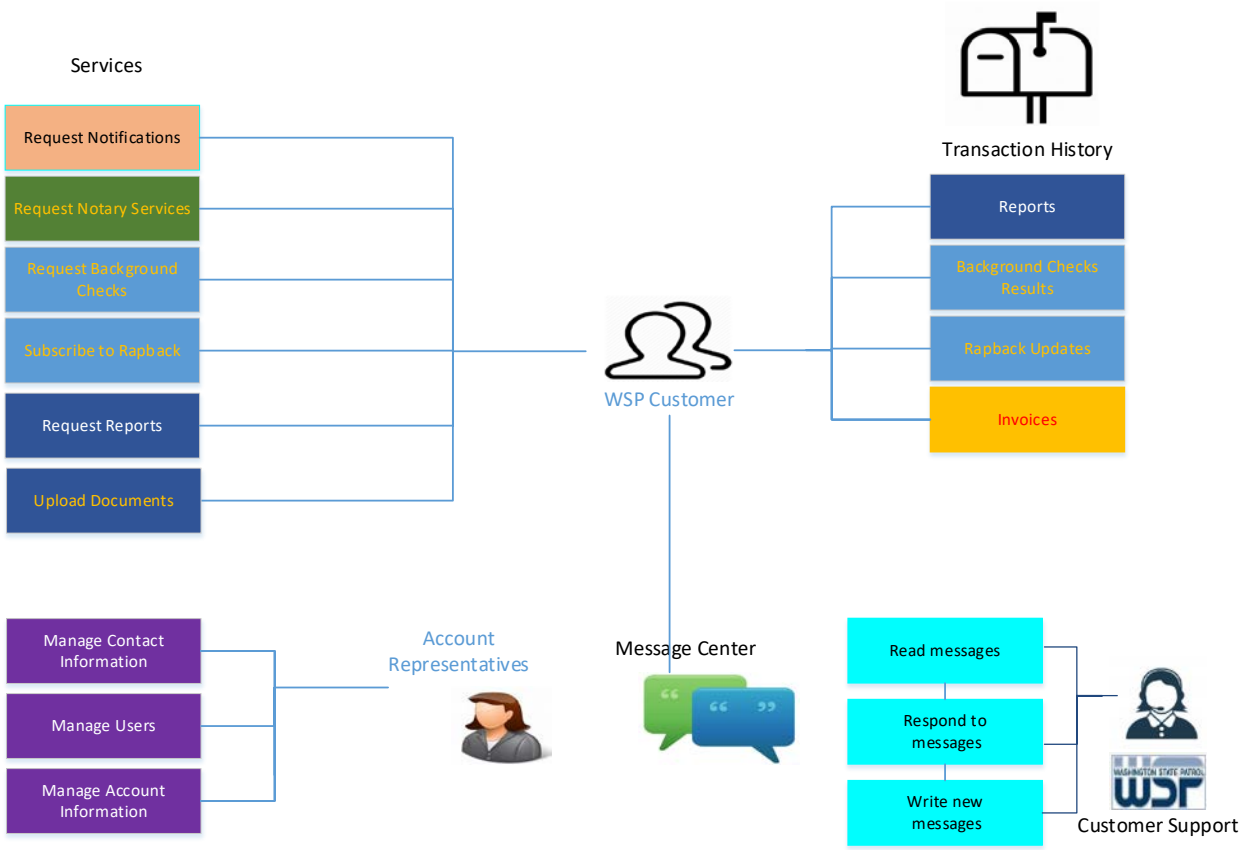
1.3.3 Business Processes Universal Requirements (S)

The following requirements apply to all procedures in all the process descriptions.

Ref ID	Requirement	Priority
UPD 01	Every CRD customer must be able to have a web portal account	Mandatory
UPD 02	Every account must have a transaction history	Mandatory
UPD 03	Every transaction history must meet CJIS standards for security	Mandatory
UPD 04	Every account must have an account representative	Mandatory
UPD 05	Every account must have a payment method	Mandatory
UPD 06	Every account must have a queue to receive, acknowledge and send messages	Mandatory
UPD 07	Every account must designate an account owner	Mandatory
UPD 08	Every account owner must supply their primary contact information	Mandatory
UPD 09	Every account must have at least one user	Mandatory
UPD 10	Every user must be uniquely identified	Mandatory
UPD 11	Every user id must be secured with a CJIS compliant password	Mandatory
UPD 12	Every user must be able create and maintain their password	Mandatory
UPD 13	Every user must have a valid registered email address	Mandatory
UPD 14	Every user must be assigned at least one account role (See Appendix A – Account Roles)	Mandatory
UPD 15	The system must support role based security to determine access to tasks, data, and documents for each user.	Mandatory
UPD 16	The system must allow every user to access their account via the internet through a CJIS compliant interface.	Mandatory
UPD 17	The system must provide a platform for CRD to securely communicate with their customers via messages and notifications, email or other methods specified in their contact information.	Mandatory
UPD 18	The system must support subscription services.	Mandatory
UPD 19	Customers must be able to subscribe for Rapback services.	Mandatory
UPD 20	Customers must be able to subscribe to have their ABIS responses sent to their transaction history.	Mandatory
UPD 21	Customers must be able to request online NDOB background checks.	Mandatory
UPD 22	Customers must be able to select and run authorized reports.	Mandatory

UPD 23	The system must support allowing customers to choose the format reports are rendered in (html, pdf, excel, or csv) and retaining those preferences.	Mandatory
UPD 24	The system must support users retrieving background check results from their transaction history.	Mandatory
UPD 25	The system must support users retrieving, printing, and downloading reports from their transaction history.	Mandatory
UPD 26	The system must support users retrieving, printing, and downloading invoices from their transaction history.	Mandatory
UPD 27	The system must support users retrieving ABIS responses from their transaction history.	Mandatory
UPD 28	The system must support notification services and notify users via email.	Mandatory
UPD 29	The system must allow the waiving of fees for a transaction	Mandatory
UPD 30	The system must be integrated with the Customer Management functions and data in WASIS. (via API)	Mandatory
UPD 31	The system must be integrated to with the Account and Financial management services in WASIS (via API)	Mandatory
UPD 32	The system must be integrated with billing services in WASIS to support end of month billing and accounting activities (via API).	Mandatory
UPD 33	The system must log users out of the system automatically after a set length of time of inactivity has occurred (this will comply with CJIS).	Mandatory
UPD 34	The portal must be isolated from code changes to WASIS and WACIC	Mandatory
UPD 35	The system must be integrated to interface with WSP Document Management Services (via API).	Mandatory
UPD 36	The system must support an integrated folder structure for the uploading of documents by customers	Mandatory
UPD 37	The system must support the secure uploading of documents by customers into designated locations	Mandatory

1.3.4 Business Processes High Level Portal Processes



1.4 Account Management (S)

Every CRD customer must have a web portal account. There are two types of accounts:

Public – Customers establish and maintain their Accounts. There may be one or more users for each account, but the user who sets up the account is automatically designated as Account Owner and Account Representative when the system creates it.

Administered Accounts – In order to establish the account the customer must make a formal request to WSP and WSP must approve the request. The administered account is established for the customer by the WSP Administrator and then notifies the customer to complete the account setup.

The work processes documented within Account Management include:

- Create an Account
- Maintain an Account
- Deactivate/Reactivate an Account
- Delete an Account

Business Process Detail Description

1.4.1 Process Description

Public customers establish and maintain their accounts. Administrated Accounts require submission of a formal request by the Account Owner that must be approved by WSP. The WSP Administrator establishes the account and then notifies the Account Representative to complete the setup. Every account has an Account Owner, at least one Account Representative and at least one Account User. As part of establishing the account, the system creates the Account's transaction history and message queue. The WSP Administrator can deactivate or reactivate passwords to restrict access to an account. The System may delete accounts in a purge process based on a predetermined set of rules.

1.4.2 Actor / System

Actor	Goal
Public User	Establishes and maintains their account.
WSP Administrator	Establishes Administered Accounts once request for account is approved by WSP. Notifies Account Representative to complete the setup. Activates and deactivates accounts.
Account Owner	The human being who is legally responsible for actions associated with this account. This individual authorizes actions such as change of account representative. They are identified on the request to setup Administered Accounts and require the submission of a new request to change.
Account Representative	Account Representatives may be granted broad administrative rights to manage the account or restrictive

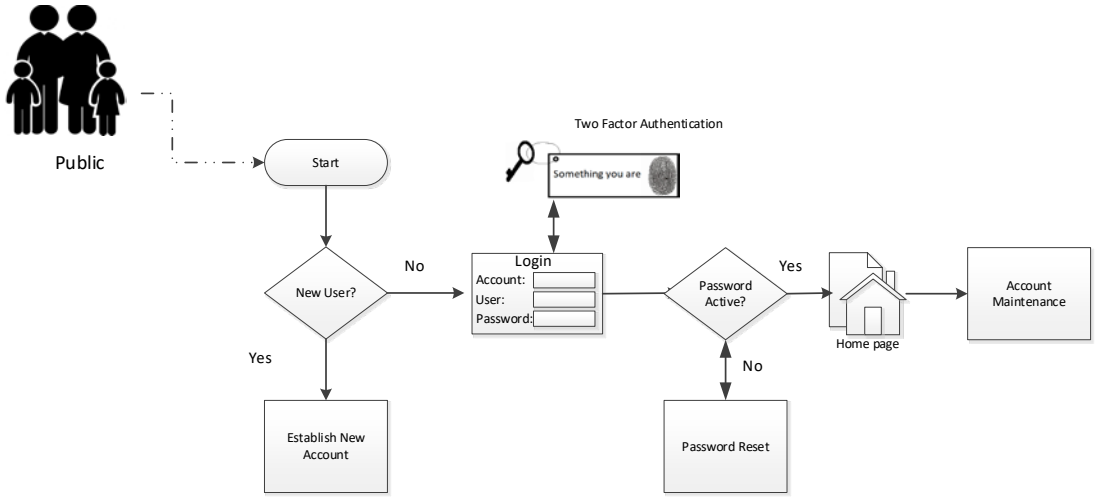
	rights based on the submitted request. For a single account the Account Representatives may have different administrative rights granted.
Account User	Accesses the services, messages, and transaction history items for the account
System	**Purpose**
System	Enforces the rules for account creation and maintenance.

1.4.3 Triggering Events

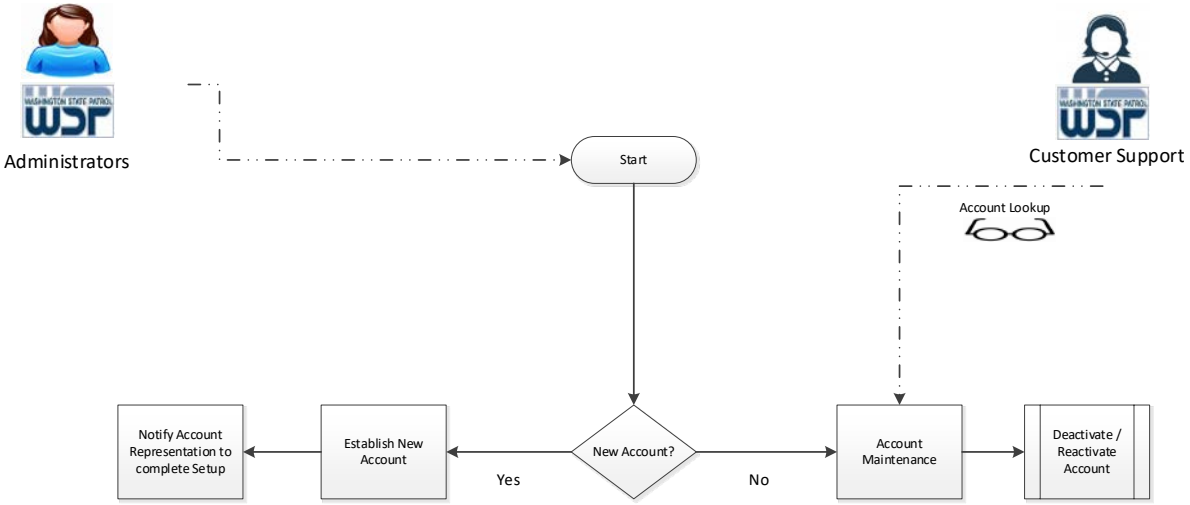
Event Description
Public user creates an account
Public user changes account information
Public user requests to have their account reactivated
WSP Administrator creates an Administered Account
WSP Administrator changes an Administered Account
WSP Administrator deactivates an account
WSP Administrator reactivates an account
System identifies an inactive public account and force user to re-authenticate
System identifies an account to be deleted and deletes it as part of a purge process
CRD Staff runs a report to list accounts and account information

1.4.4 Process Steps

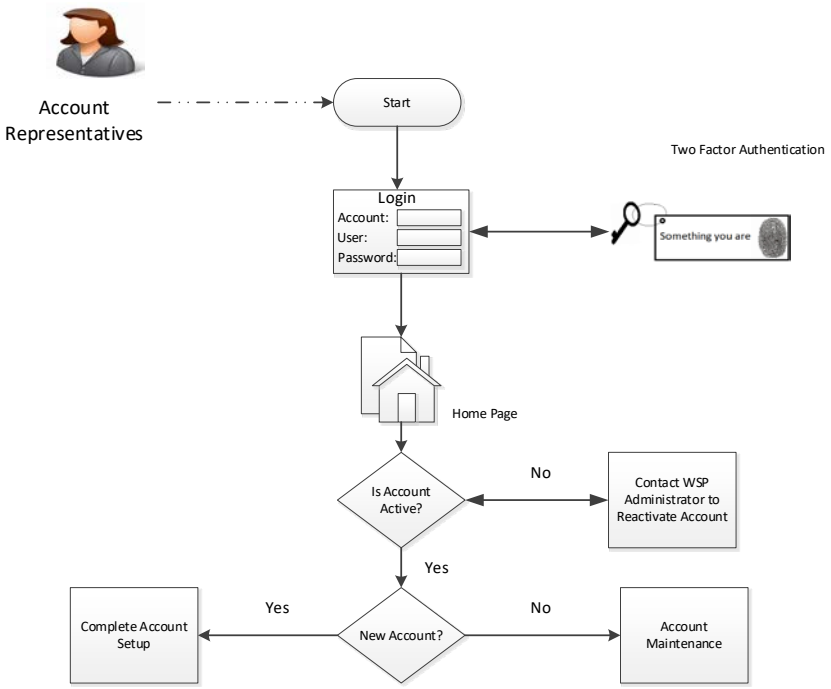
Public Accounts



Administered Accounts



Administered Accounts



1.4.5 Functional Requirements

Ref #	Requirement	Priority
ACM 01	All accounts must meet CJIS security standards for automatic logoff due to inactivity, password complexity, two factor authentication and password updates.	Mandatory
ACM 02	Public customers establish and self-maintain their accounts using the Web Portal.	Mandatory
ACM 03	The system must distinguish public accounts from Administered Accounts.	Mandatory
ACM 04	The system must designate public users as the Account Owners of their accounts.	Mandatory
ACM 05	The system designates public users as the Account Administrator and Account Representative for their accounts.	Mandatory
ACM 06	The system assigns public account users a “public account” account role. (See Appendix A – Account Roles)	Mandatory
ACM 07	The system assign the interface type for public accounts (see Appendix B – Interface Types)	Mandatory
ACM 08	Public accounts are always pre-paid accounts “for profit”.	Mandatory

Ref #	Requirement	Priority
ACM 09	Public accounts are assigned the payment method of “Pre-Paid”	Mandatory
ACM 10	Public account role must be able to perform NDOB background checks. (See Appendix A – Account Role)	Mandatory
ACM 11	Public account role receive “conviction only” data responses for their background check queries. (See Appendix D - Types of Background Check Results).	Mandatory
ACM 12	Public account role must be able to receive and view background check responses in their transaction history. (See Appendix A – Account Role)	Mandatory
ACM 13	Public accounts must be able to request Notary Services	Mandatory
ACM 14	When the password for a Public Account is deactivated the user must re-authenticate using the password process [ACM 01].	Mandatory
ACM 15	WSP Administrators must be able to establish and perform maintenance on Administered Accounts.	Mandatory
ACM 16	Only WSP Administrators assign payment methods for Administered Accounts. (see Appendix C)	Mandatory
ACM 17	Only WSP Administrators assign type of interface used by Administered Accounts (see Appendix B)	Mandatory
ACM 18	Only WSP Administrators designate whether Administered Accounts are “For Profit” or “Non-Profit”.	Mandatory
ACM 19	Only WSP Administrators designate whether “Non-Profit” accounts are “501C3” or not.	Mandatory
ACM 20	Only WSP Administrators assign fees to Administered Accounts	Mandatory
ACM 21	Only WSP Administrators assign fingerprint reasons to Administered Accounts (see Appendix F)	Mandatory
ACM 22	Only WSP Administrators assign types of transactions (TOT) to Administered Accounts (see Appendix I)	Mandatory
ACM 23	Only WSP Administrators authorize Administered Accounts to request Notary Services.	Mandatory
ACM 24	Only WSP Administrators assign type of background check responses permissible for Administered Accounts (see Appendix D)	Mandatory
ACM 25	Only WSP Administrators assign an agency ORI as a customer number for Administered Accounts.	Mandatory

Ref #	Requirement	Priority
ACM 26	WSP Administrators must be able to deactivate and reactivate any account. Deactivation is intended to force Customer to contact CRD in order to reactivate the account.	Mandatory
ACM 27	Only WSP Administrators designate the valid account roles for Administered Accounts (see Appendix A)	Mandatory
ACM 28	CRD Staff must be able to easily lookup and locate Administered Accounts information in order to provide customer support. A lookup with a variety of search criteria must be offered.	Mandatory
ACM 29	The system must log all account actions including the date/time, user id, account, IP address, action (establish account, change account, disable account, enable account, delete account)	Mandatory

1.5 Account Owner Management (S)

Every web portal account must have an Account Owner. The account owner is the human being that is legally responsible for the requests made. It is primarily a legal delineation that is cited here for the sake of completeness. The purpose of the Account Owner is the same regardless of the type of web portal account, the difference is how the account owner is designated for each type of web portal accounts:

Public Accounts – Establish and maintain their accounts. The user who establishes the account is designated as Account Owner at time of account creation and is the legal owner of the account.

Administered Accounts – When the customer submits their request to establish an account with WSP, they designate an individual who will be the legal owner of the account. When the WSP Administrator establishes the account they assign the Account Owner. This individual is the only person that can authorize WSP Administrators to make certain changes to the Account. A change of account owners requires submission of a formal written request to WSP.

The work processes documented within Account Owner Management include:

- Create Account Owner
- Maintain Account Owner

Business Process Detail Description

1.5.1 Process Description

The user who sets up a public account is designated as the owner of their account. The formal request to establish an Administered Account with WSP includes the name of the account owner. The WSP Administrators assigns the account owner as part of the establishment of the administered account. The owner is the considered the legal owner of the account. The customer must submit a formal request to WSP for the WSP Administrator to change the account owner. Users should have visibility to the account owner, but only the WSP Administrator has any rights to change the Account Owner.

1.5.2 Actor / System

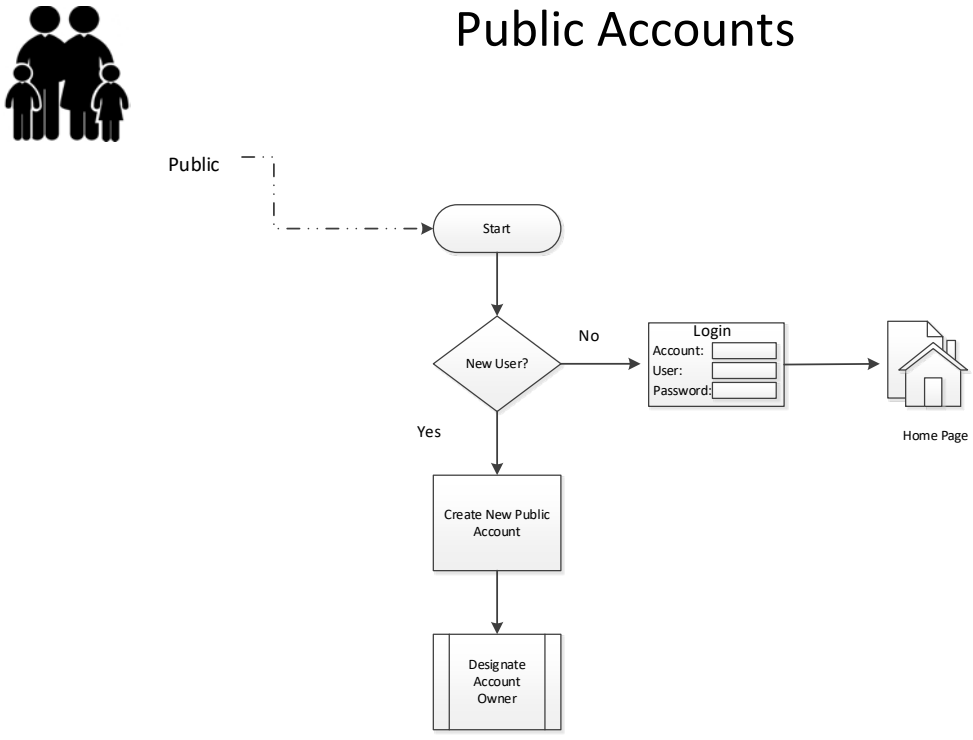
Actor	Goal
Public User	Is designated as the account owner when they establish their account
WSP Administrator	Receives a formal request to establish an account and assigns the account owner when establishing the account. Will change the owner if they receive authorization from the customer.
Account Owner	The person designated as the owner of the account.
Account Representative	N/A
Account User	N/A
System	**Purpose**

System	Enforces the rules for Account Owner management

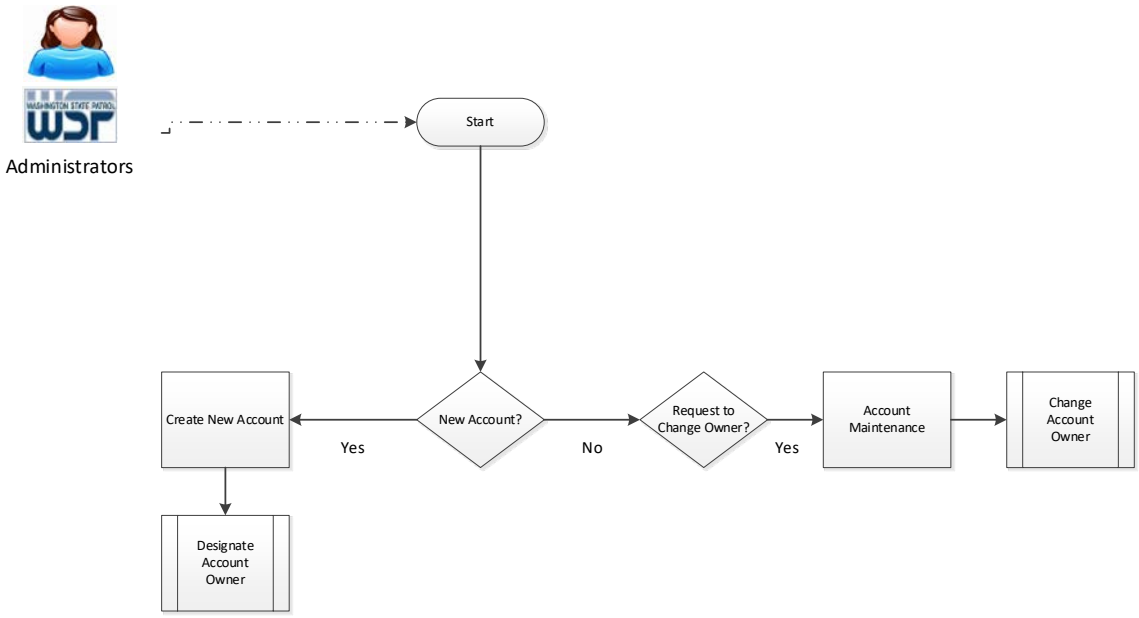
1.5.3 Triggering Events

Event Description
Public user establishes their account and is automatically designated Account Owner
CRD receives a request to setup an account, the WSP Administrator sets up the account and designates the Account Owner
CRD receives a formal request to change the Account Owner. The WSP Administrators changes the Account Owner
CRD Staff run a report listing Administered Accounts and Account Owners so they can insure that the accounts owners are all current.

1.5.4 Process Steps



Administered Accounts



1.5.5 Functional Requirements

Ref #	Requirement	Priority
AOM 01	The system will designate public users as the owners of their account when the account is created.	Mandatory
AOM 02	WSP Administrators will designate the Account Owner when creating an Administered Account.	Mandatory
AOM 03	The WSP Administrators can maintain and change Account Owners for Administered Accounts	Mandatory
AOM 04	CRD Staff must be able to easily lookup and locate Account Owners. The lookup must offer a variety of search criteria.	Mandatory
AOM 05	The system must log all Account Owner actions including the date/time, user id, account, IP address, action (create Account Owners, change Account Owners, delete Account Owners.)	Mandatory

1.6 Account Representative Management (S)

Every web portal account must have at least one designated Account Representative. The account representative is granted certain administrative privileges to the account. How Account Representatives are designated and maintained vary by account type. There are two types of web portal accounts:

Public Accounts – Customers establish and maintain their accounts. When the customer establishes their account the system designates them as Account Representative and grants them privileges as the Account Representative for a public account.

Administered Accounts – When the customer submits their request to establish an account with WSP, they designate at least one individual who serves as Account Representative. When the WSP Administrator establishes the account they designate the Account Representative and grant them privileges as Account Representative. These privileges can include: the maintenance of non-primary contact information, authority to designate and maintain users, administrative rights to account's transaction history.

The work processes documented within Account Representative Management include:

- Establish Account Representatives
- Maintain Account Representatives
- Grant Account Representatives authority
- Disable Account Representatives
- Delete Account Representatives

Business Process Detail Description

1.6.1 Process Description

When the public establishes an account the system designates them as the Account Representative and grants them public Account Representative privileges. WSP Administrators have authority to assign Account Representatives for Administered Accounts and grant privileges to them. These privileges control what tasks the Account Representative can perform. Different Account Representatives on the same account may be granted different privileges. The intention is that once Account Representatives are configured for an Administered Account they become the primary managers of the account with privileges that can include authority to create, maintain and delete users from the account and delete items from the transaction history.

1.6.2 Actor / System

Actor	Goal
Public User	Is granted privileges to: delete items from their transaction history and maintain their contact information. Acts as the Account Representative for the account.
WSP Administrator	Assigns the Accounts Representative and grants privileges to them based on request from Account Owner.

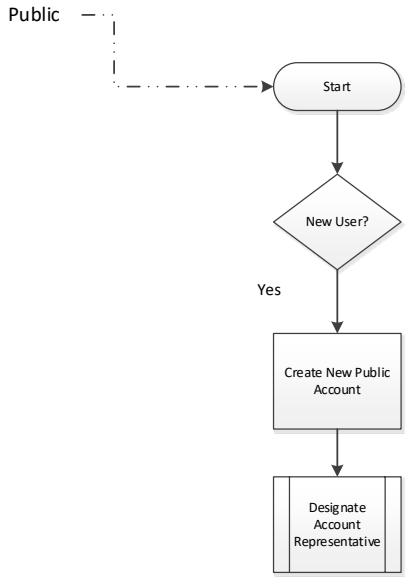
Account Owner	Submits request to establish an Administered Account and designates the Account Representatives for the account.
Account Representative	Is assigned as an Account Representative by the WSP Works based on privileges granted by the WSP Administrator.
Account User	N/A
System	**Purpose**
System	Enforces the rules for Account Representative management

1.6.3 Triggering Events

Event Description
The process of the public customer establishing their account includes them being automatically designated Account Representative
CRD receives a request to setup an account, the WSP Administrator assigns the Account Representatives and grants them privileges.
WSP Administrators may grant an Account Representative the privilege to create and maintain users for the account.
The WSP Administrator may grant the Account Representatives the privilege to maintain transaction history for the account
The WSP Administrator adds, modifies, disables Account Representatives
The system runs a purge that deletes disabled Account Representatives if certain parameters are met
CRD Staff runs reports to list Account Representatives by account.

1.6.4 Process Steps

Public Accounts



Administered Accounts

1.6.5 Functional Requirements

Ref #	Requirement	Priority
AAM 01	The system designates public users as the Account Representatives for their accounts	Mandatory
AAM 02	WSP Administrators designate and manage Account Representatives for Administered Accounts.	Mandatory
AAM 03	WSP Administrators grant Account Representatives authority to create users for the account. Other Account Representatives on the same account may not be granted authority to create users.	Mandatory
AAM 04	WSP Administrators grant Account Representatives rights to maintain the account's transaction history (read, print, download, delete).	Mandatory
AAM 05	WSP Administrators can add Account Representatives	Mandatory
AAM 06	WSP Administrators can update the authorities granted Account Representatives	Mandatory
AAM 07	WSP Administrators can disable Account Representatives	Mandatory
AAM 08	CRD Staff must be able to easily lookup and locate Account Representatives. The lookup must offer a variety of search criteria.	Mandatory
AAM 09	The system must log all Account Representative actions including the date/time, user id, account, IP address, action (create Account Representatives, change Account Representatives, disable Account Representatives, add Account Representatives.)	Mandatory
AAM10	The system can purge disabled Account Representatives if they match certain criteria	Mandatory

1.7 Account Role Management (S)

Account Roles group tasks performed by customers and provide a table driven means of granting privileges for a common sets of those tasks. An individual user may be assigned more than one account role. WSP Administrators determine what account roles are appropriate for an Administered Account and once they have assigned those roles to the account, an Account Representative can assign account roles to individual users from the list of valid account roles. Each role grants specific privileges to the user that should provide them with the access they need to perform their work on the portal. Every account must have at least one valid account role and every web portal user must be assigned *at least one* account role.

Public Accounts – When user establishes their account the user is automatically assigned the account role. The public account role will grant the use the privileges they need to administer their account and transaction history.

Administered Accounts – The WSP Administrator assigns the authorized roles to Administered Accounts. Each user created must be assigned *at least one* authorized role.

The work processes documented within Account Role Management include:

- Maintain Account Role
- Disable Account Role
- Delete Account Role
- Assign Account Roles to an Account
- Change Account Roles for an Accounts

Business Process Detail Description

1.7.1 Process Description

When a public user creates an account the system will automatically assign their public account role. This role grant the privileges for a user of a public account are granted. In the process of establishing the Administered Account the WSP Administrator determines which Account Roles are valid for this account. For example: the role of ABIS Coordinator would only be applicable for organizations that prove ABIS information to WSP. There must be at least one account role assigned to an account. Every user must be assigned at least one account role from those account roles that are authorized for the account. The system uses the account roles to determine the tasks a user can perform and what data they can view. WSP Administrators manage the account roles assigned to Administered Accounts and if necessary can disable/enable account roles. Account Roles are pre-defined and table driven. See Appendix A for examples of the expected Account Roles.

1.7.2 Actor / System

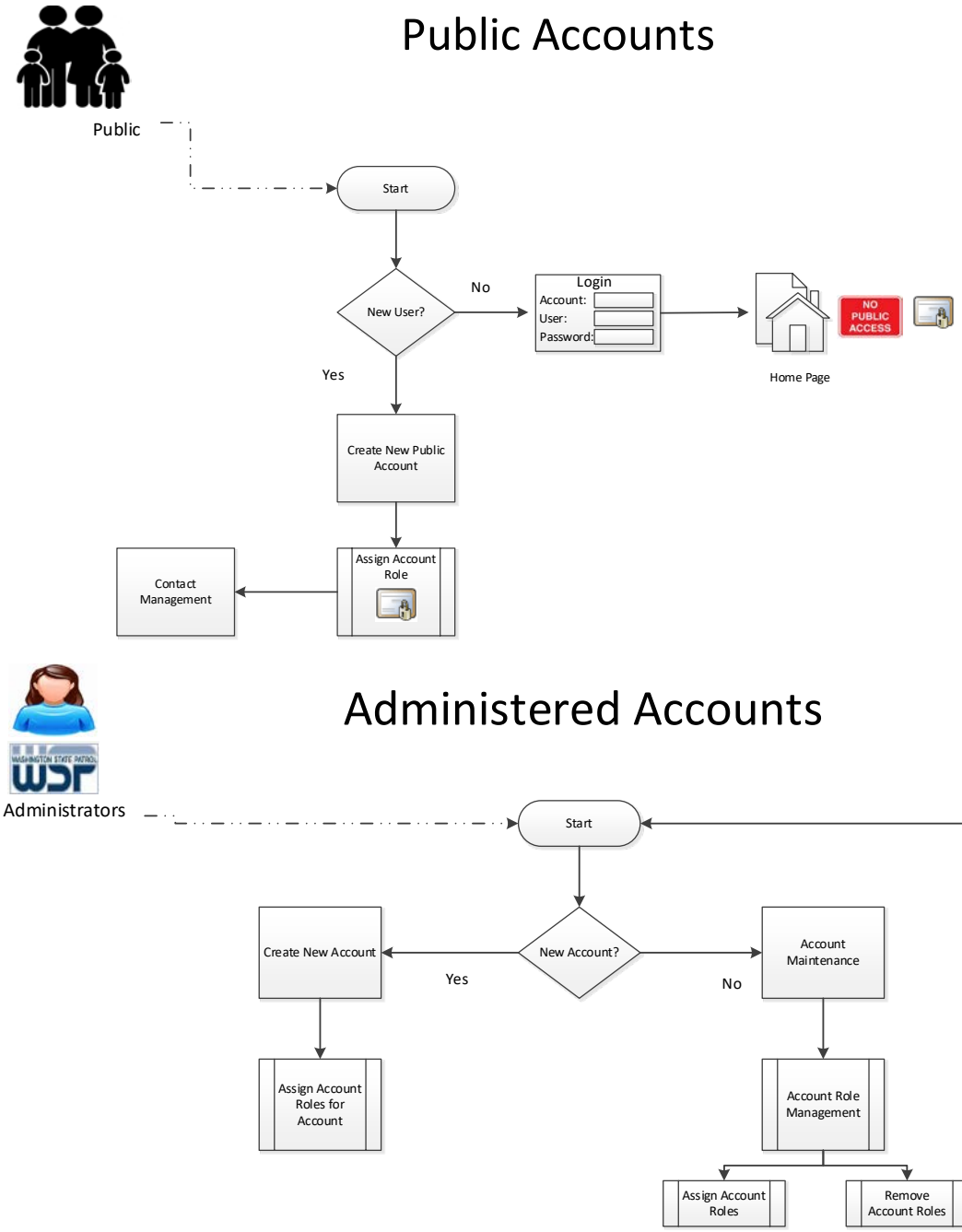
Actor	Goal
Public User	System assigns Account Role when account created
WSP Administrator	Assigns and maintains authorized Account Roles for Administered Accounts. Assigns Account Roles when maintaining Account Users.

Account Owner	Authorizes Account Representatives and Account Roles
Account Representative	May assign Account Roles to Account Users if authorized to maintain Account Users.
Account Users	System uses Account Role to determine the tasks the user can perform and the data they can see.
System	**Purpose**
System	Enforces the rules for Account Role management

1.7.3 Triggering Events

Event Description
Public User creates an Account and Account Role is automatically assigned
The system provides a table of valid Account Roles and access as defined by CRD
WSP Administrators enable or disable Account Roles
CRD receives a request to create an Account and the WSP Administrator creates the Account, including assigning the authorized Account Roles for the account.
WSP Administrators assigns Account Roles to Account Users including Account Representatives.
Account Representatives may assign Account Roles to Account Users if they are authorized to assign Users to the Account
The System enforces that each user is assigned at least one Account Role
The System uses Account Roles to determine access to functions, documents, data and notifications for that user
CRD Staff runs reports that identify Account Users by Account Roles

1.7.4 Process Steps



1.7.5 Functional Requirements

Ref #	Requirement	Priority
ARM 01	The system maintains a table of valid Account Roles and the access associated with each.	Mandatory
ARM 02	WSP Administrators view and enable/disable Account Roles	Mandatory

Ref #	Requirement	Priority
ARM 03	The system automatically assigns an Account Role to Public Users when they create their accounts.	Mandatory
ARM 04	WSP Administrators assign Account Roles to an Account when creating Administered Accounts.	Mandatory
ARM 05	WSP Administrators add or remove Account Roles for Administered Accounts.	Mandatory
ARM 06	WSP Administrators assign at least one Account Role to each user for an Administered Account	Mandatory
ARM 07	Account Representatives authorized to add users assign at least one Account Role to each user for the account.	Mandatory
ARM 08	The system must validate that each user must have at least one Account Role assigned.	Mandatory
ARM 09	The system must use Account Roles to control access to tasks, data and services	Mandatory
ARM 10	The system must use Account Roles to control access to the transaction history	Mandatory
ARM 11	The system must use Account Roles to filter the items in the transaction history.	Mandatory
ARM 12	The system must prevent users with only disabled Account Roles from accessing services (functions, transaction histories)	Mandatory
ARM 13	The system will delete disabled Account Roles if they match pre-determined criteria.	Mandatory
ARM 15	CRD Staff must be able to easily lookup and locate Account Roles. The lookup must offer a variety of search criteria.	Mandatory
ARM 16	The system must log all Account Role Management actions including the date/time, user id, account, IP address, action (Create Account Role, change Account Role, disable Account Role, Delete Account Role.)	Mandatory

1.8 User Management (S)

Every web portal account must have *at least one* user. Each user is associated with a valid registered email address. When a user is created the system generates a unique identifier and initiates the process to establish the user's password. There are two types of web portal accounts:

Public – Create and maintain their accounts. There is must be at least one user for each account. The user provides their email address as part of account creation and the system validates the email address before initiating the creation of the account including the password.

Administered Accounts – When the WSP Administrators establish the Administered Account and create the Account Representative they create the user whose role is Account Representative. With some accounts the WSP Administrator will create all the users for account and in other cases they will authorize Account Representatives to create users. For each user the system must validate the email address before initiating their password creation.

The work processes documented within User Management include:

- Create Users
- Maintain Users
- Disable Users
- Delete Users

Business Process Detail Description

1.8.1 Process Description

When a public user creates an account the system first validates that the customer is providing a valid email address. Once the validation process is completed, the user establishes their password and the system generates a unique identifier for the user. The user is designated by the system as: the Account Owner, the Account Representative and assigns the account role. If the owner of the account wishes to change their email address, they must validate the new email address before the system can reassign them to a new email address.

When the WSP Administrator sets up an Administered Account they must designate at least one Account User who can be assigned as the Account Representative. Account user creation requires a name and initial email address and the assignment of an authorized account role. The user's initial logon initiates the email validation process. Once the email address is validated, the system can initiate the password generation process, etc.

The WSP Administrator can authorize the Account Representative with the authority to create users. Once the Account Representative is established they can add users provided they enter the name, initial email address and authorized account role. The same process applies whether the user is entered by the WSP Administrator or the Account Representative. Both can maintain names, account roles, and email addresses for users and can either enable or disable users as needed. Changes to user's email address will force the user to validate the new email address they can access the portal.

The system enforces the rules of User Management and insures that each user id remains unique in the system and all activities associated with that user id are logged and auditable. A purge routine will check all disabled user ids to determine if any meet the pre-determined deletion criteria and if so the user is deleted.

1.8.2 Actor / System

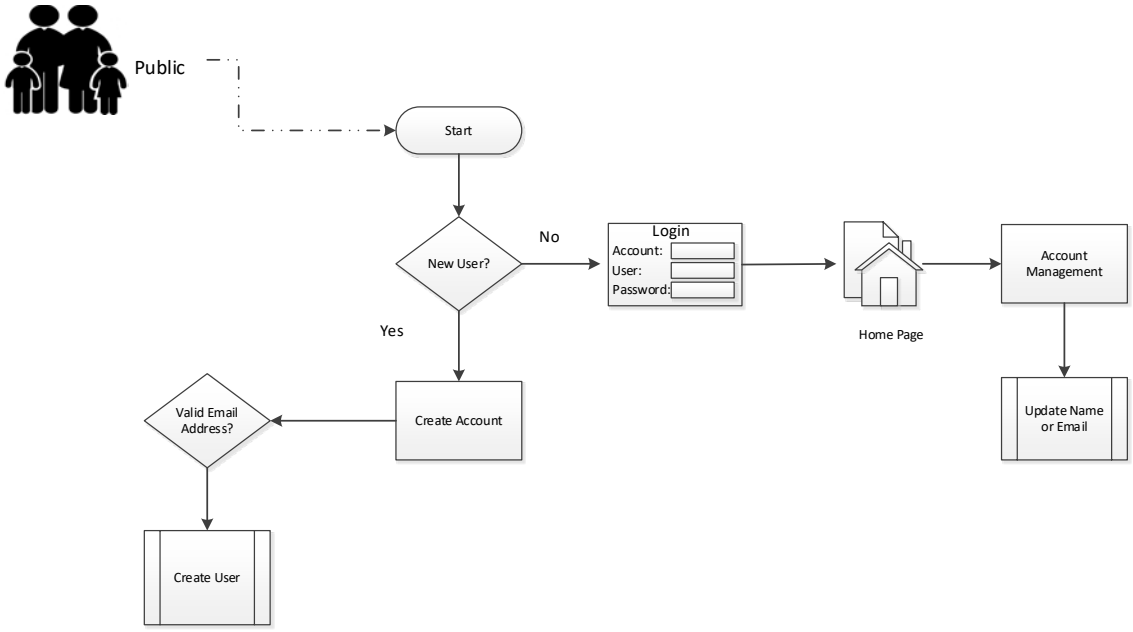
Actor	Goal
Public User	User is created when account is created.
WSP Administrator	Creates and maintains users for Administered Accounts. They authorize Account Representatives to create and maintain users.
Account Owner	Submits requests for Account Representatives and users to CRD.
Account Representative	May be authorized by the WSP Administrator to create and maintain users for an Administered Account.
Account User	Are assigned to the account and are requested to establish a password.
System	**Purpose**
System	Uniquely identifies each user. Stores user profile information for user and enforces the rules for user management.

1.8.3 Triggering Events

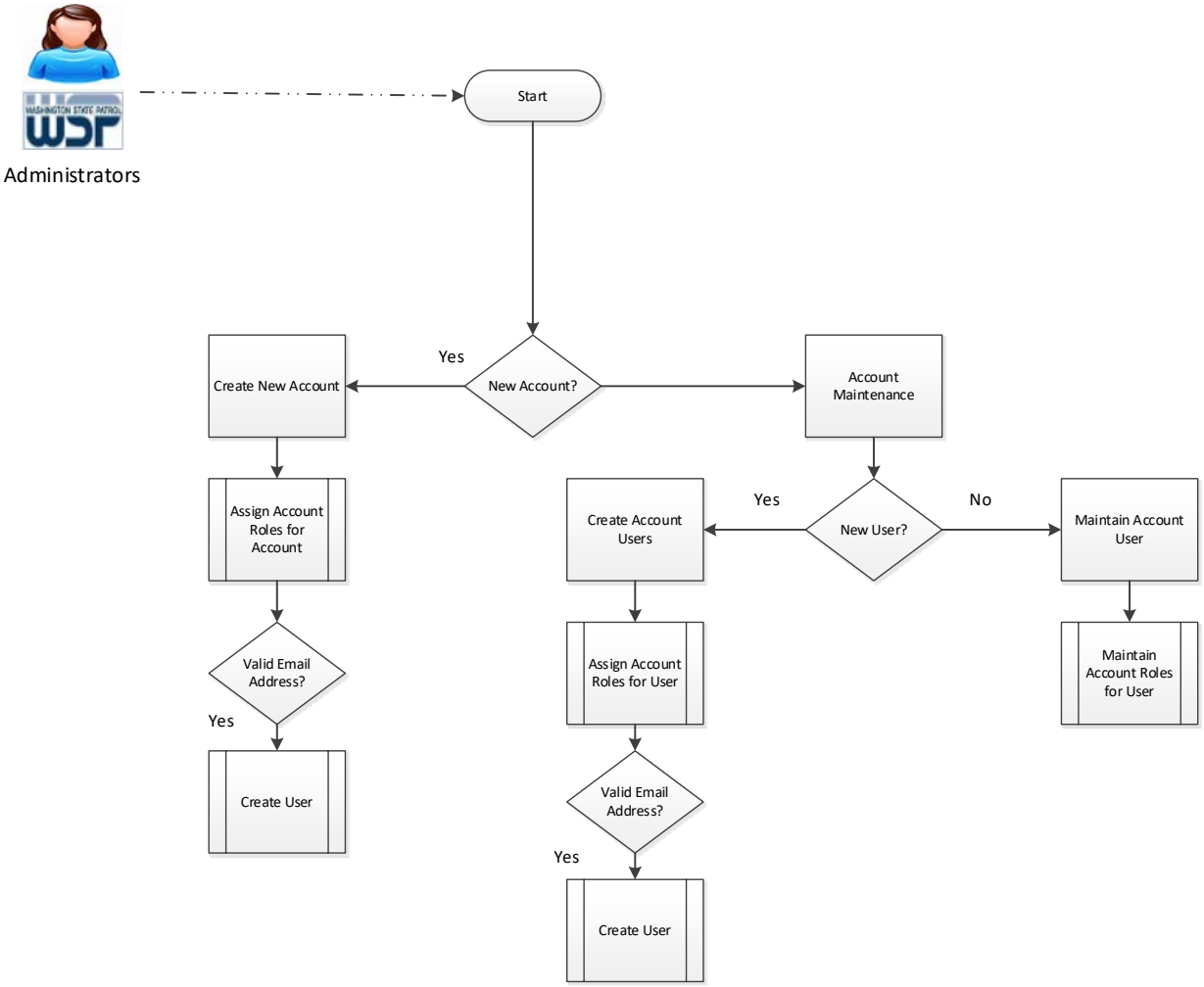
Event Description
A Public User creates an account and the user is created as part of that process
WSP Administrator creates a user for an Administered Account
WSP Administrator updates a user for an Administered Account
WSP Administrator disables a user
Account Representative creates a user for an Administered Account
Account Representative updates a user for an Administered Account
Account Representative disables a user for the Administered Account
The System enforces the rules for User Management
The System identifies disabled users and if they meet pre-determined criteria they are deleted
The System validates that the email address for a user is valid
CRD Staff runs a report to locate users by account

1.8.4 Process Steps

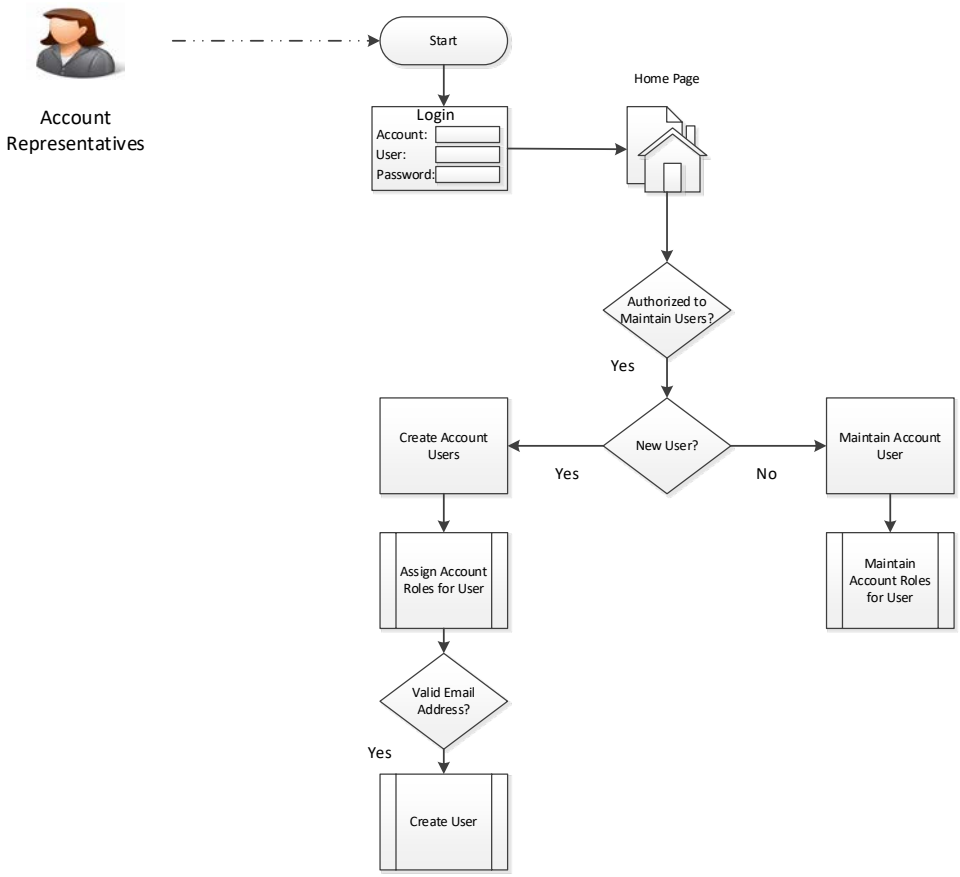
Public Accounts



Administered Accounts



Administered Accounts



1.8.5 Functional Requirements

Ref #	Requirement	Priority
AUM 01	The system must uniquely identify each user	Mandatory
AUM 02	Every user must have a valid email address	Mandatory
AUM 03	The system must validate the email address provided before creating a user and registering the email	Mandatory
AUM 04	The system must create a user for each public account when it is created	Mandatory
AUM 05	The system must assign the public Account Role to each user of a public account	Mandatory
AUM 06	Each user must provide a name (First, Last) with their user profile	Mandatory
AUM 07	WSP Administrators are able to create users for Administered Accounts	Mandatory

Ref #	Requirement	Priority
AUM 08	The system must enforce that each user is assigned a valid Account Role for their Administered Account.	Mandatory
AUM 09	WSP Administrators may grant Account Representatives authority to create users. (i.e., the same account may have Account Representatives authorized to create users and Account Representatives who are not).	Mandatory
AUM 10	Authorized Account Representatives must be able to create users for their account.	Mandatory
AUM 11	WSP Administrators must be able to disable users	Mandatory
AUM 12	Authorized Account Representatives must be able to disable the users for their account.	Mandatory
AUM 13	CRD Staff must be able to easily lookup and locate users by account. The lookup must offer a variety of search criteria.	Mandatory
AUM 14	The system must log all User Management actions including the date/time, user id, account, IP address, action (Create Users, Update Users, Disable Users)	Mandatory
AUM 15	The systems must be able to identify disabled users and if they meet certain criteria they can be deleted	Mandatory

1.9 Password Management (S)

Every web portal user is required to have a CJIS compliant password in order to access their account. There are two types of web portal accounts:

Public Accounts –The user creates and maintains their account including their password. As part of account creation the system notifies the user to create their password.

Administered Accounts – WSP Administrators and designated Account Representatives create users for the account. As part of the user creation the system notifies the user to create their password. The Account User then maintains their password.

Once the password is established the system must validate passwords each time users access the system. The system must follow CJIS rules for structure and validation of passwords. The system must provide a process to help users remember their password and reset their password if so required.

When WSP Administrators or Account Representatives re-enable disabled users the user will be prompted to reset their password as part of the process.

Passwords are time sensitive and the system enforces expiration rules for passwords at preset intervals. Users can sign up to be notified in advance of the expiration of their passwords.

The work processes documented within Password Management include:

- Creating a password
- Changing a password
- Validating a password
- Expiring a password

Business Process Detail Description

1.9.1 Process Description

Each user logs into the web portal using an account, user id and password. All users create and maintain their password in order to access their account. Public users create their passwords when they create their accounts. Users for an Administered Account are notified automatically to create their passwords when their user is created for an account by the WSP Administrator or Account Representative. The system enforces the rules for the creation, structure, expiration, and validation of passwords.

1.9.2 Actor / System

Actor	Goal
Public User	Creates their password when they create their account and maintains their password.
WSP Administrator	When creating users for Administered Accounts the system notifies users to create passwords.
Account Representative	When creating users for an Administered Account the system notifies the user to create a password.

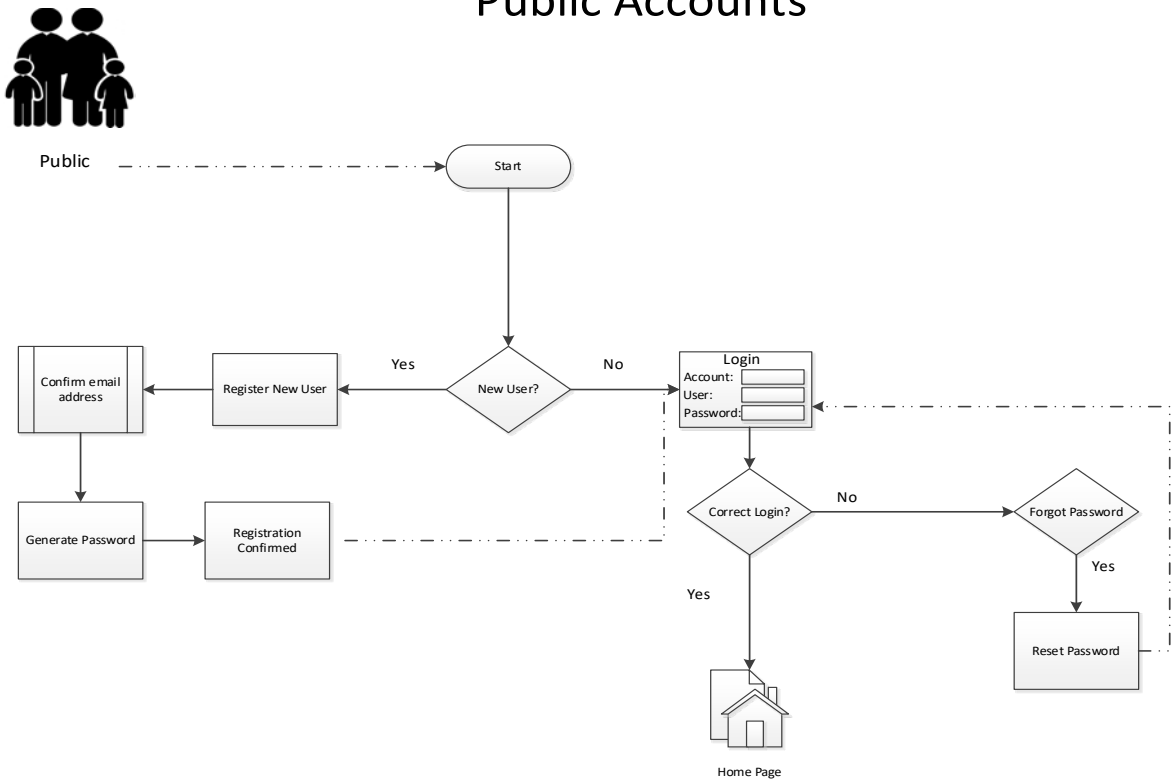
Account User	Creates their password and maintains their password.
System	**Purpose**
System	Validates, Retains, and Enforces Password use

1.9.3 Triggering Events

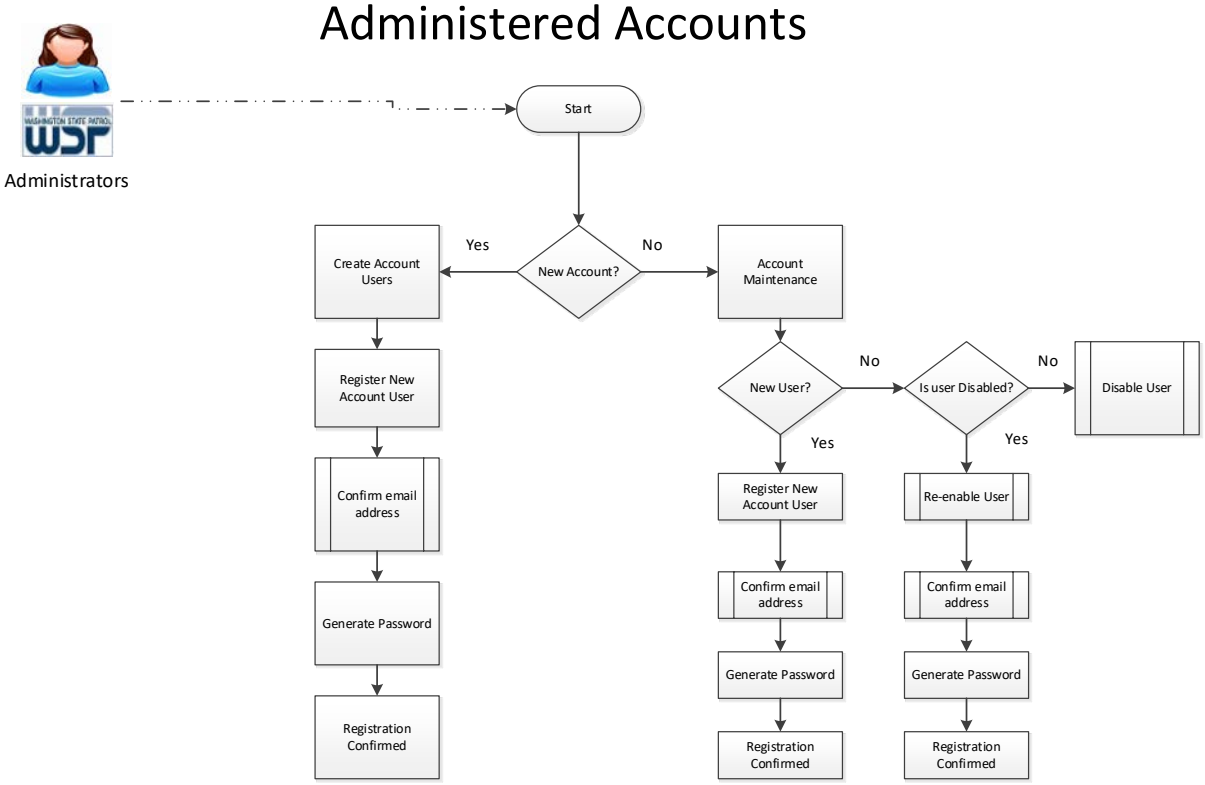
Event Description
Public user creates an account and is prompted to create a password.
The WSP Administrator creates a user for an Administered Account and the system notifies the user to log in and create a password.
An Account Representative creates a user for an Administered Account and the system notifies the user to log in and create a password.
A user forgets their password and received prompts to help them remember it.
A user needs to change their password.
A user fails to enter the correct password and receives an error message
The system identifies that a password that is going to expire and sends notification to the user.
The system identifies that a password has met its expiration date. It disables the user id and sends notification to the user.
The system identifies that a user has failed to enter the correct password multiple times. The password is disabled and the user receives notification on whom to contact to reset the account.
The WSP Administrator or the Account Representative enables a disabled password and the system notifies the user to log in and create a new password.

1.9.4 Process Steps

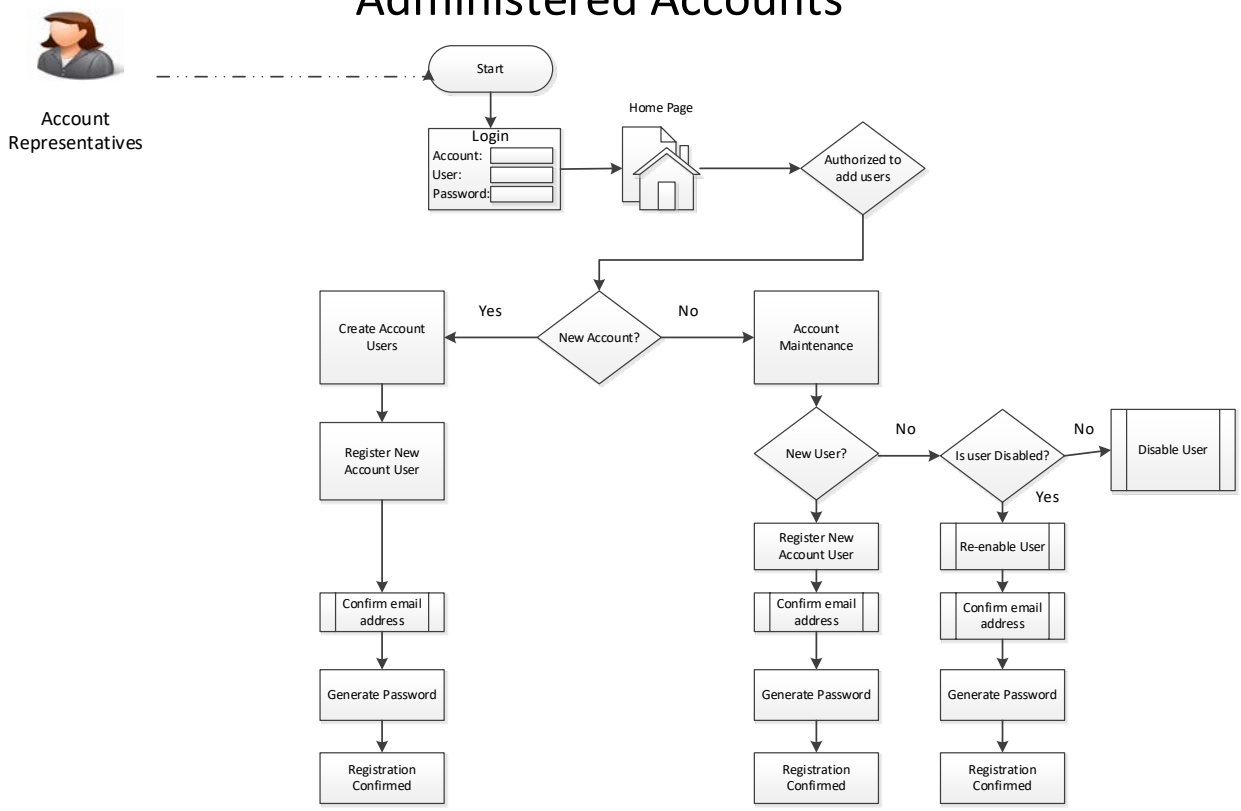
Public Accounts



Administered Accounts

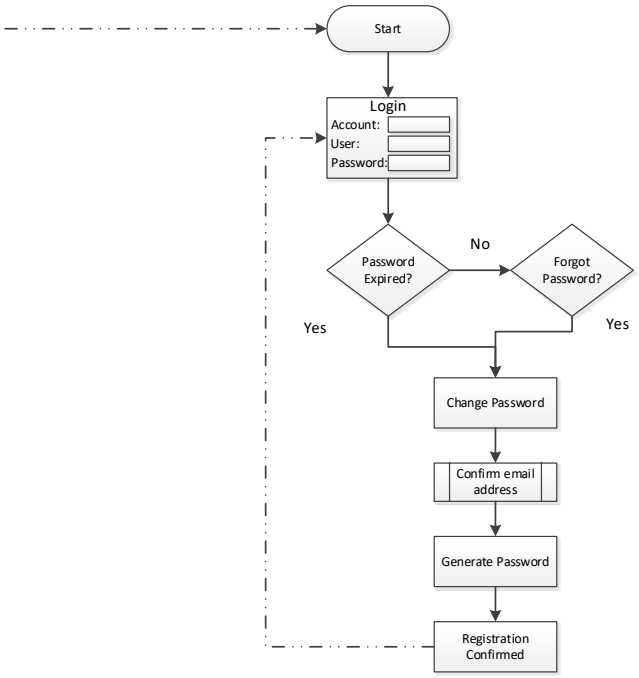


Administered Accounts



Administered Accounts

Account Users



1.9.5 Functional Requirements

Ref #	Requirement	Priority
PWM 1	The system must enforce CJIS password standards on password creation (length and composition of password).	Mandatory
PWM 2	The system must enforce CJIS standards on retention of passwords (encryption, etc.)	Mandatory
PWM 3	The system must enforce CJIS standards for the duration of passwords. Forcing users to change their password at proscribed intervals and expiring passwords that have not been used in a set period of time.	Mandatory
PWM 4	The system must provide a means for users to change their password.	Mandatory
PWM 5	The system must disable users after a set number of failed attempts to enter the correct password.	Mandatory
PWM 6	Public users create and maintain their passwords.	Mandatory
PWM 7	The system will notify users created by WSP Administrators or Account Representatives to login and create a password.	Mandatory

Ref #	Requirement	Priority
PWM 8	The system must allow WSP Administrators and designated Account Representatives the ability enable disabled users.	Mandatory
PWM 9	The system must notify users re-enabled by WSP Administrators or Account Representatives to login and create a password.	
PWM 10	The system must display error messages that inform the user in the case that their password is invalid, number of tries allowed, password expired, or other error messages necessary so that user can maintain their password.	Mandatory
PWM 11	The system must meet auditing standards for WaTech, WSP and CJIS for password management	Mandatory
PWM 14	The system should send notifications to users at regular intervals before their passwords expire.	Should Have
PWM 15	The system should send notifications to users when their passwords expire.	Should Have
PWM 16	The system should sending notifications to users whose user id has been disabled because of multiple failed attempts.	Should Have
PWM 17	The system must provide reporting of disabled users and those with expired passwords.	Mandatory
PWM 18	CRD Staff must be able to easily lookup and locate the status of a user (enabled, disabled, expiring password). The lookup must offer a variety of search criteria.	Mandatory
PWM 19	The system must log all password actions including the date/time, user id, account, IP address, action (change password, invalid password entered, etc.)	Mandatory

1.10 Contact Management (S)

Every web portal account must supply primary contact information in order to create the account. Contact Management covers both primary and non-primary contact information for each account. There are two types of web portal accounts and each has different primary contact information:

Public – Create and maintain their account including their contact information. The user fills in the required contact information when creating the account and maintains their primary contact information.

Administered Accounts – Primary contact information is provided with the account request. The WSP Administrator enters and maintains the primary contact information for the Account. Contact information for each Account Role assigned to the Account is maintained by the Account Representative.

The work processes documented within Contact Management include:

- Create primary contact information
- Maintain primary contact information
- Create contact information for an account role
- Change contact information for an account role

Business Process Detail Description

1.10.1 Process Description

When a public user creates an account they provide their name and email address. They maintain this primary contact information. Contact Management allows them to also provide physical and mail addresses, phone numbers, and identify their preferred method of delivery for notarized documents.

The primary contact information for an Administered Account is maintained by the WSP Administrator and any changes should be authorized by the account owner.

Account Representatives maintain the contact information for account roles assigned to the account. Contact Management allows them to maintain physical and mail addresses, email addresses, phone numbers and identify their preferred method of delivery for notarized documents.

CRD staff use Contact Management to locate the appropriate contact information for a customer.

The system enforces the rules of contact management.

1.10.2 Actor / System

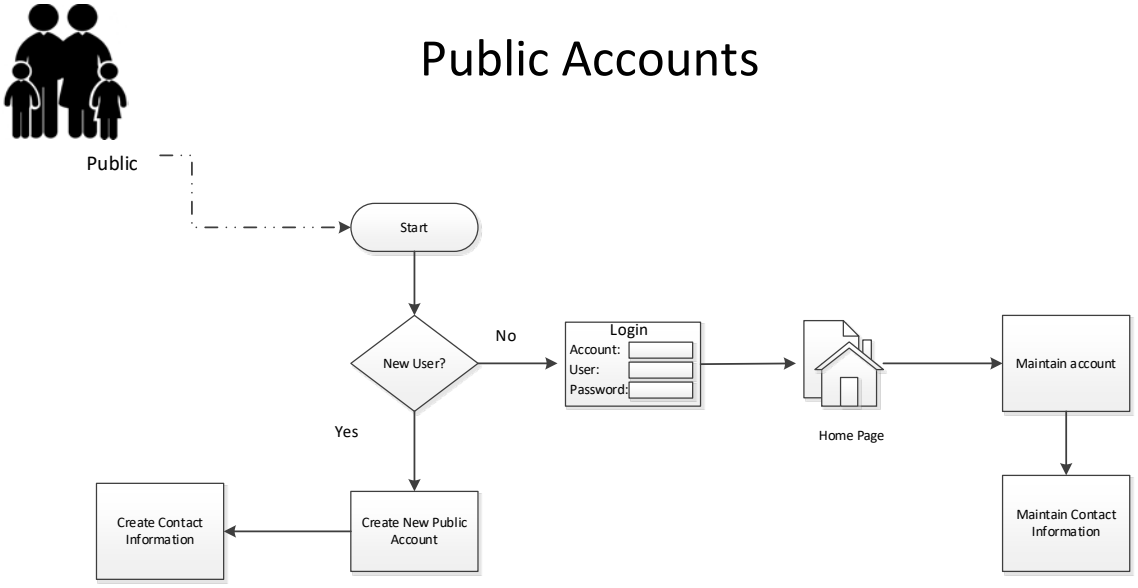
Actor	Goal
Public User	Creates and maintains their contact information
WSP Administrator	Creates and maintains primary contact information for administered accounts
Account Owner	Authorizes changes to primary contact information for the account they are the designated owner

Account Representative	Maintains all other account role contact information for Administered Account
Account User	N/A
CRD Staff	Uses lookup or reports to find and review contact information for customers
System	**Purpose**
System	Enforces the rules for contact management

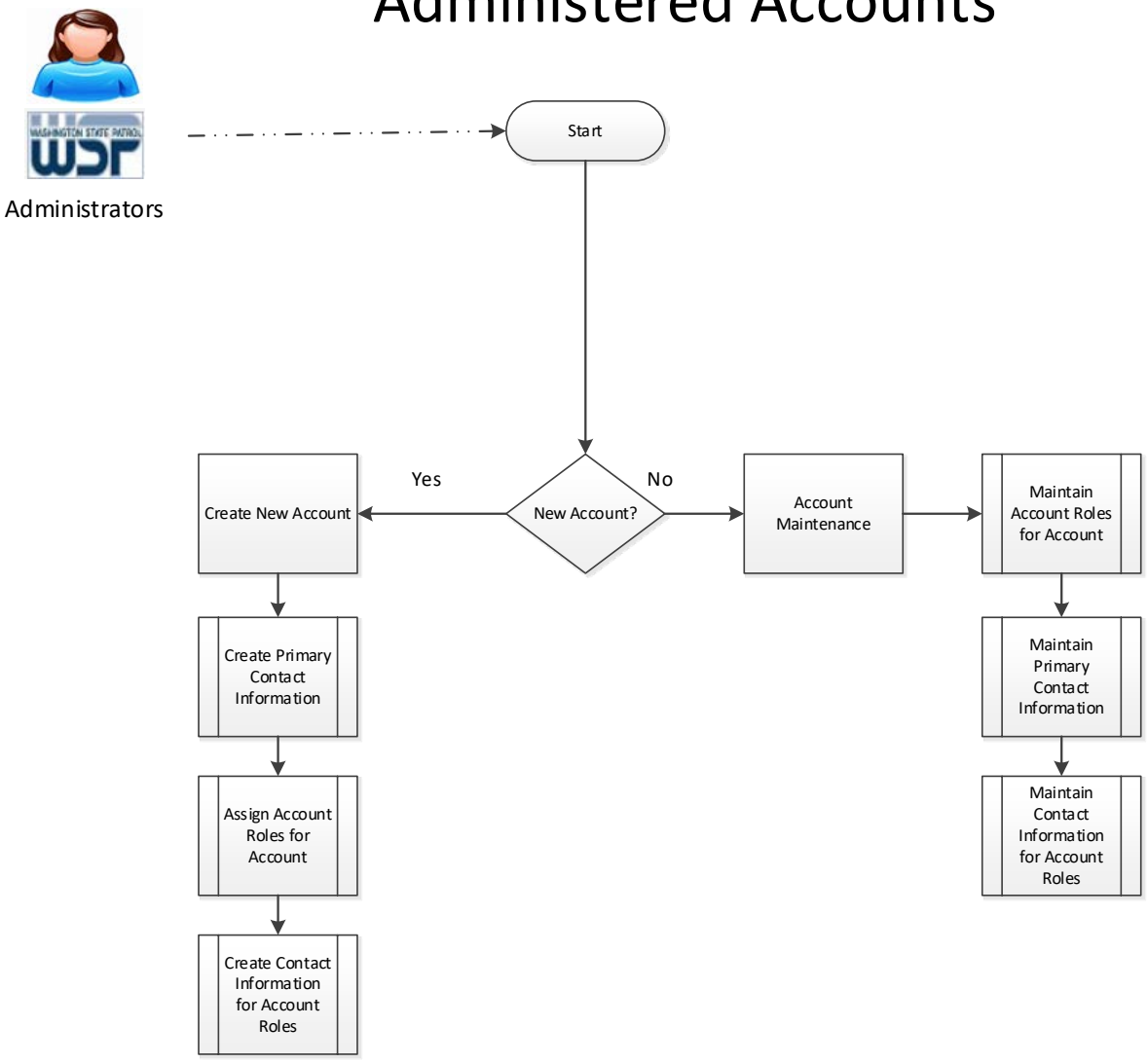
1.10.3 Triggering Events

Event Description
Public user creates an account and must provide primary contact information
Public user updates their contact information
WSP Administrator enters primary contact information for Administered Accounts
WSP Administrator updates primary contact information for Administered Accounts
Account Representative enters contact information for Account Roles for an Administered Account
Account Representative changes contact information for Account Roles for an Administered Account
The System enforces editing and validation rules for contact management
CRD Staff runs a report to retrieve contact information for accounts
CRD Staff looks up contact information for accounts

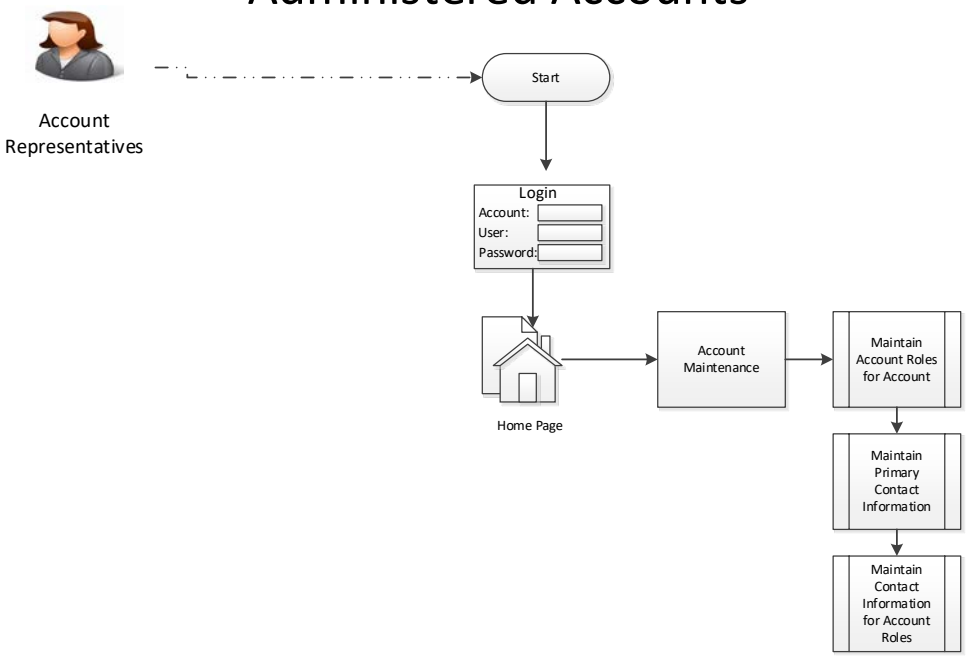
1.10.4 Process Steps



Administered Accounts



Administered Accounts



1.10.5 Functional Requirements

Ref #	Requirement	Priority
CMM 01	Every account must provide primary contact information when it is created	Mandatory
CMM 02	The system must edit and validate contact information for all accounts. (Primary Contact Name, Primary Email Address, Contact Name, Physical Address, Mail Address, Email Address, etc.)	Mandatory
CMM 03	Public accounts create and maintain their contact information	Mandatory
CMM 04	Mandatory Primary Contact Information is Name and Email Address. Non-Mandatory information includes: Name, Address, Phone #, Email, Preferred means of contact, etc.	Mandatory
CMM 05	WSP Administrators create and maintain primary contact information for Administered Accounts.	Mandatory
CMM 06	Mandatory Primary Contact Information for Administered Accounts include: Account Name, Owner Name, Owner Email, Physical Address, Mailing Address, Central Phone #, Fax#, Email, Website, ORI, etc.	Mandatory
CMM 07	Contact information for Assigned Account Roles includes: Name, Address, Phone #, Email, Preferred means of contact, etc.	Mandatory

Ref #	Requirement	Priority
CMM 08	Account Representative create and maintain contact information for the Account Roles for their Administered Account.	Mandatory
CMM 09	CRD Staff must be able to easily lookup and locate contact information for an Account or groups of Accounts that meet specific criteria.	Mandatory
CMM 10	The system must log all contact management actions including the date/time, user id, account, IP address, action (create contacts, change contacts, delete contacts.)	Mandatory

1.11 Payment Management (S)

Every web portal account must have a payment method in order to be enabled. There are two types of web portal accounts:

Public Accounts – Create and maintain their accounts. These account are assigned the payment method of "Pre-Paid" (Credit Cards) when the Account is created. They maintain their payment information through a gateway to third party software. Payment activity is tracked and reported through the third party service.

Administered Accounts – WSP Administrators create and manage the payment method for Administered accounts. They assign either "Billed" or "Not Billed" as payment methods to accounts. Payment activity is tracked and reported to the WASIS system using an API. The WASIS system will generate invoices for "Billed" accounts in a pdf format that will be posted to their transaction history.

The work processes documented within Payment Method include:

- Assign a Payment Method
- Change a Payment Method
- Waive fees for a Transaction

Business Process Detail Description

1.11.1 Process Description

All accounts have a payment method. Public users are assigned their payment method when they create their accounts. Third-party software then maintains their credit card information. Administered Accounts are assigned payment methods by the WSP Administrator. Account activity is tracked by the system and reported to the WASIS system. The WASIS system will generate invoices for "Billed" accounts that are posted to the account's transaction history.

1.11.2 Actor / System

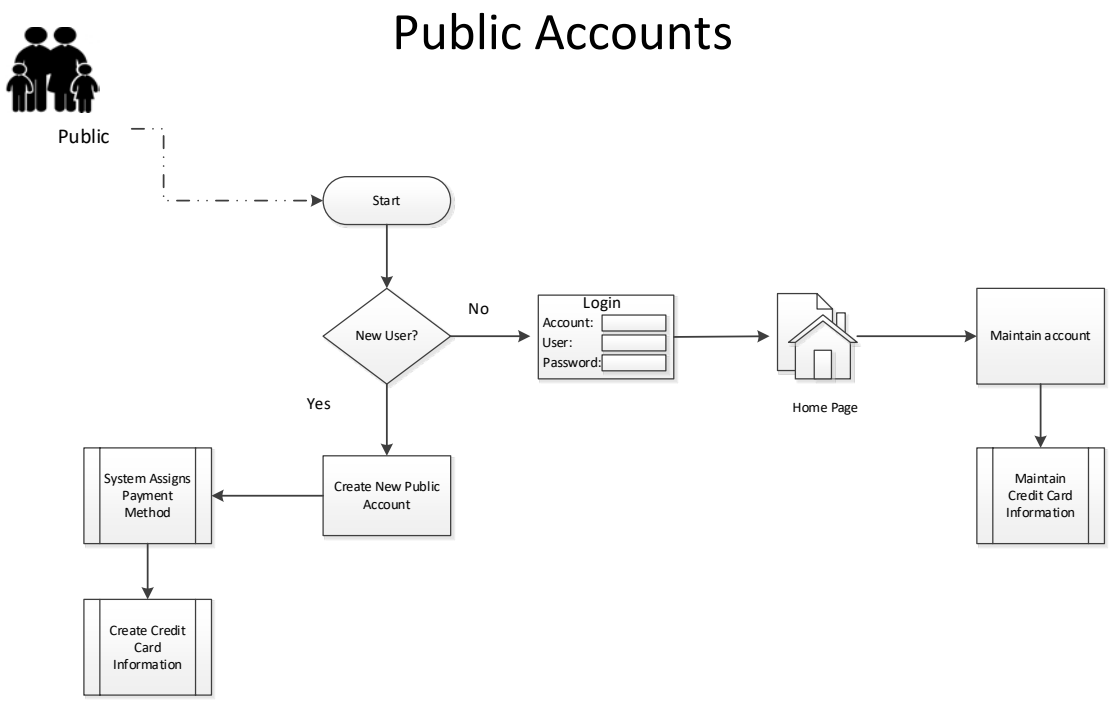
Actor	Goal
Public User	Is assigned the payment method of Pre-Paid (Credit Cards). Uses external 3rd party software to maintain credit card information.
WSP Administrator	Creates and maintains payment method for Administered Accounts
Account Owner	Authorizes the payment method for the account they own
CRD Staff	Look up payment information for customers
System	**Purpose**

System	Uses payment method to determine how payment for services is managed for account and transmits payment activity to WASIS.
Credit Card Processing	External 3rd Party interface for credit card processing

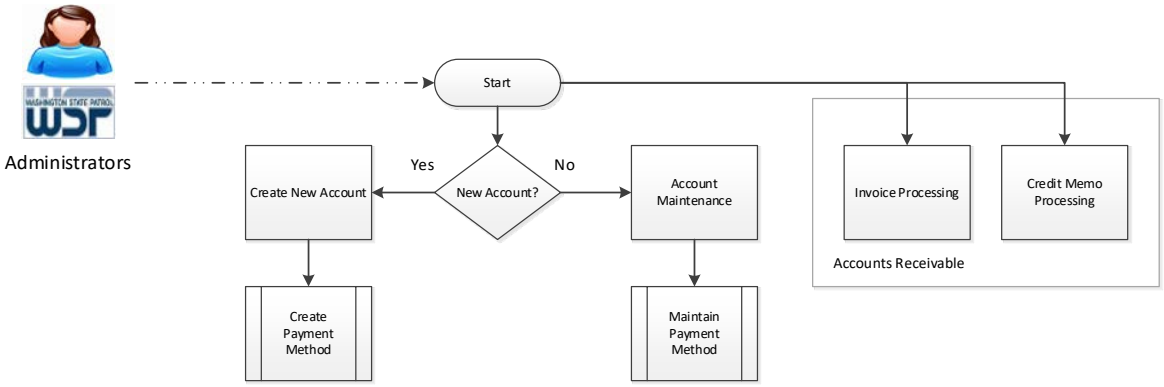
1.11.3 Triggering Events

Event Description
Public user creates an account and payment method is assigned. User is routed to third party service where credit card information is entered and verified
Public user requests to change credit card and is routed to third party services
The WSP Administrator assigns a payment method for a Administered Account
The WSP Administrator changes the payment method for a Administered Account
CRD staff runs processes in WASIS to issue invoices for “billed” accounts
Web portal payment activities are transmitted to with account and financial functions in WASIS via an API.
CRD staff run a report or look up information on customers by payment method and can track activity for customers

1.11.4 Process Steps



Administered Accounts



1.11.5 Functional Requirements

Ref #	Requirement	Priority
PMM 01	The system will assign the payment method of Pre-Paid (Credit Cards) when a public account is created.	Mandatory
PMM 02	The system must support the use of third-party pass-through for the creation and maintenance of Credit Card payments for Public Users.	Mandatory
PMM 03	The system must prevent Public Users from performing background checks when their credit card has expired.	Mandatory
PMM 04	WSP Administrators must assign a payment method when an account is created.	Mandatory
PMM 05	WSP Administrators must be able to change the payment method for an Account.	Mandatory
PMM 06	The system must transmit payment activity in the web portal to the WASIS.	Mandatory
PMM 07	CRD Staff must be able to easily lookup and locate accounts by payment method. The lookup must offer a variety of search criteria.	Mandatory
PMM 08	The system must log all payment actions including the date/time, user id, account, IP address, action (create payment method, change payment method, and delete payment method.)	Mandatory

1.12 Billing and Revenue Management (S)

Every CRD customer must have a web portal account. The WSP Web Portal is only expected to transmit payment activities to the WASIS system. The management of financial accounts including invoicing and credit memos is a part of WASIS and not considered part of the portal. The information is included so that the bidder has a complete picture of the integrated services. There are two types of accounts:

Public - Create and maintain their accounts. These accounts are assigned a payment method of pre-pay. Billing and Revenue Management do not applies to public accounts.

Administered Accounts – The WSP Administrator creates and maintains the account. These accounts are assigned a payment method of either billed or not billed. The transmission of payment information to WASIS is the only part of Billing and Revenue Management that applies to the Web Portal.

The work processes documented within Billing and Revenue Management include:

- Request Invoices
- Generate Invoices

Business Process Detail Description

1.12.1 Process Description

Each administered account has a payment method. These are either "billed" or "not billed." Billing and Revenue Management is for managing "billed" accounts. Each billed account has the Account Role of "Billing Management" automatically assigned for managing the billing. Each "billed" account needs a user assigned the Account Role of "Billing Management."

1.12.2 Actor / System

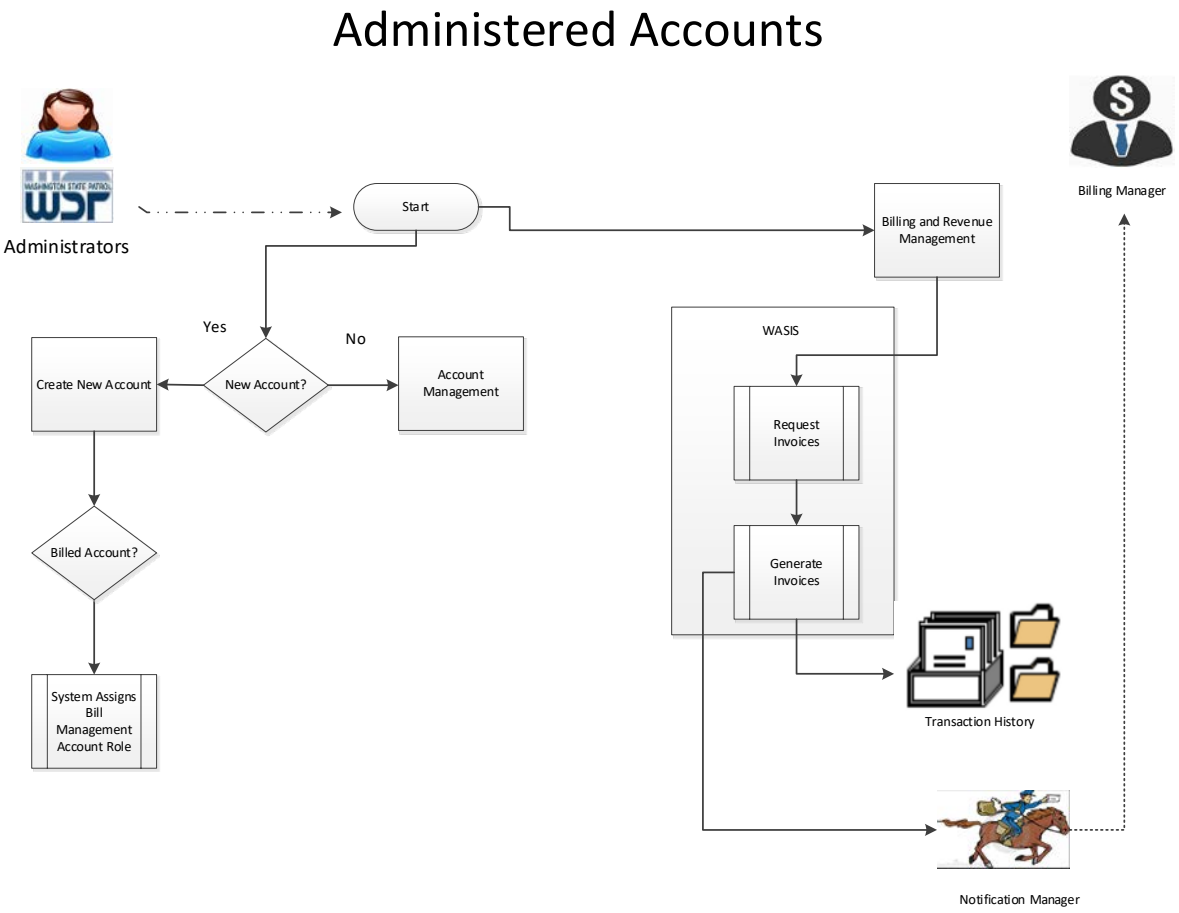
Actor	Goal
Public User	N/A
WSP Administrator	Creates and maintains "billed" accounts. Can assign the role of Billing Management to a user. Requests invoices.
Account Owner	Authorizes changes to billing information for account. Identifies who the Billing Manager is for the account.
Account Representative	Can change contact and notification information for the 'Billed Management' role. Can assign the role of Billing Management to a user.
Billing Management Role	User with role of "Billing Management" can access invoices in transaction history
System	**Purpose**
The System	Assigns the role of "Billing Management" when a "billed" account is created. [*Generates invoices in WASIS based on*

	requests from BGU]. Posts invoices (pdf format) to transaction history. Sends notifications to “Billing Management”.

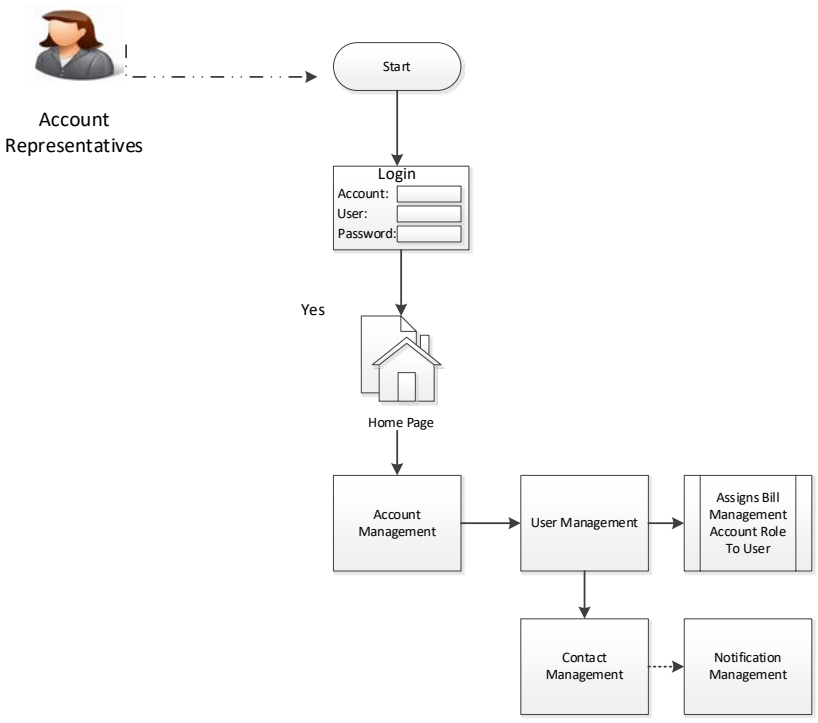
1.12.3 Triggering Events

Event Description
The WSP Administrator creates a “billed” account
The System assigned the role of “Billing Management” to a “billed” account
The WSP Administrator assigns the role of “Billing Management” to a user of a billed account
The Account Representative assigns the role of “Billing Management” to a user of a billed account.
The Account Representative or Account User sets up Notification Services for the role of “Billing Management”.
The Account User with the role of “Billing Management” received notification that there is a new invoice posted in their transaction history.
The Account User with the role of “Billing Management” accesses the transaction history for the account and retrieves their invoices.
[*BGU staff uses WASIS to requests an invoice or invoices*]
[*WASIS generates the invoices*]
The system routes the invoices to the appropriate transaction histories and sends notifications to the “billing management” role (if setup)

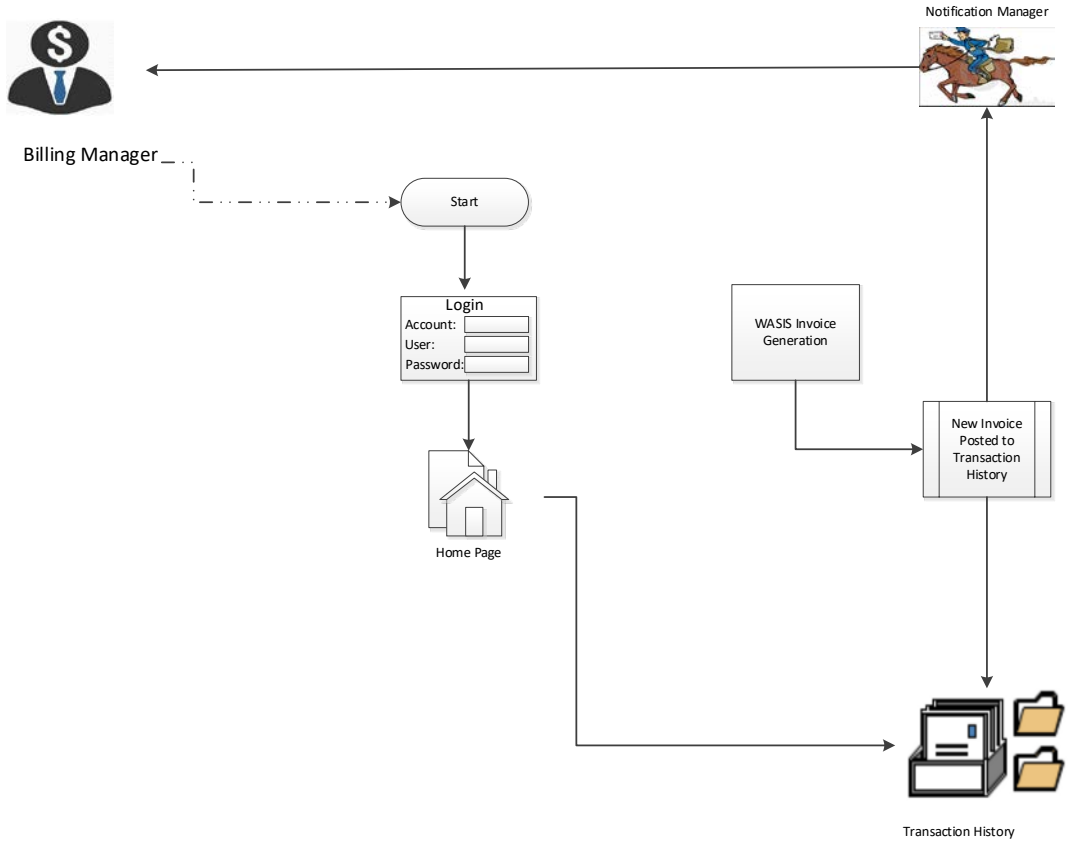
1.12.4 Process Steps



Administered Accounts



Administered Accounts



1.12.5 Functional Requirements

Ref #	Requirement	Priority
BRM 01	The system must post an invoice generated in WASIS (pdf) to transaction history.	
BRM 02	The system must track the costs for billed and non-billed customers for their activities and transmit them to WASIS through API.	
BRM 03	The system must route invoices to the transaction history for the account	Mandatory
BRM 04	The system send a notification for the “billing manger” role that is the designated for the account when an invoice is posted to the transaction history.	Mandatory
BRM 05	CRD Staff must be able to easily confirm that invoices have been posted to transaction history and that notifications have been sent.	Mandatory

Ref #	Requirement	Priority
BRM 06	The system must log all posting of invoices and notifications of invoice postings actions including the date/time, user id, account, IP address, action (request invoice, request duplicate invoice)	Mandatory

1.13 Transaction History Management (S)

Every web portal account has a transaction history. The transaction history is where documents and reports are posted. There are two types of web portal accounts:

Public Accounts – Create and maintain their accounts. The system creates the transaction history when the user creates the Account. The User is the Account Representative who owns and maintains the transaction history.

Administered Accounts – The system creates the transaction history when the WSP Administrator creates the account. The Account Representative owns and maintains the transaction history. Account Roles control access the transaction history and access to items in the transaction history.

The work processes documented within Transaction History Management include:

- Transaction History Creation
- Transaction History Access
- Delete Transaction History Items

Business Process Detail Description

1.13.1 Process Description

Each account on the web portal has a transaction history. Every user has access to an account but not necessarily a transaction history. Account Representatives own and maintain their transaction histories. This means they can access all items in the transaction history including be able to delete items. They are notified if storage is being exceeded or items are going to be purged by the system. Access to the Administered Account transaction histories and items in the transaction history is determined by account roles. Items posted in the transaction history may include: responses to NDOB searches, results from Fingerprint based background checks, invoices and various reports.

1.13.2 Actor / System

Actor	Goal
Public User	When the public creates an account the system creates the transaction history for the account. As Account Representative they are granted full rights to their transaction history and full access to all items in transaction history.
WSP Administrator	When creating an Administered Account the system creates the transaction history for the account. The WSP Administrator assigns the Account Representative who the system grants full rights to the transaction history and all the items in the transaction history. The roles assigned the account determine access to items in the transaction history.

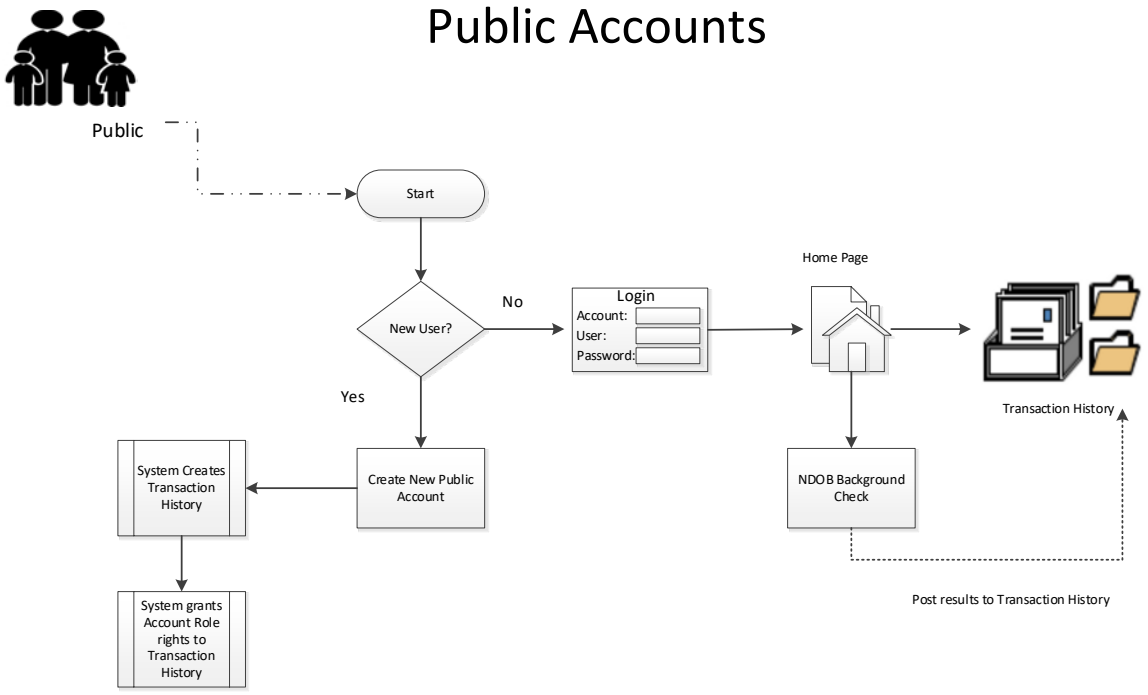
Account Representative	As Account Representative they are granted full rights to their transaction history and full access to all items in transaction history. The roles they assign to users determine access to the items in the transaction history.
Account User	The Account User access to items in transaction history is controlled by the Account Roles assigned them.
System	**Purpose**
System	When an account is created the system creates a transaction history for the account. The system enforces the rules for accessing and maintaining the transaction history. It manages the size of the transaction history. It sends notifications to users when items are added to the transaction history and notifies Account Representatives when the transaction history is full.

1.13.3 Triggering Events

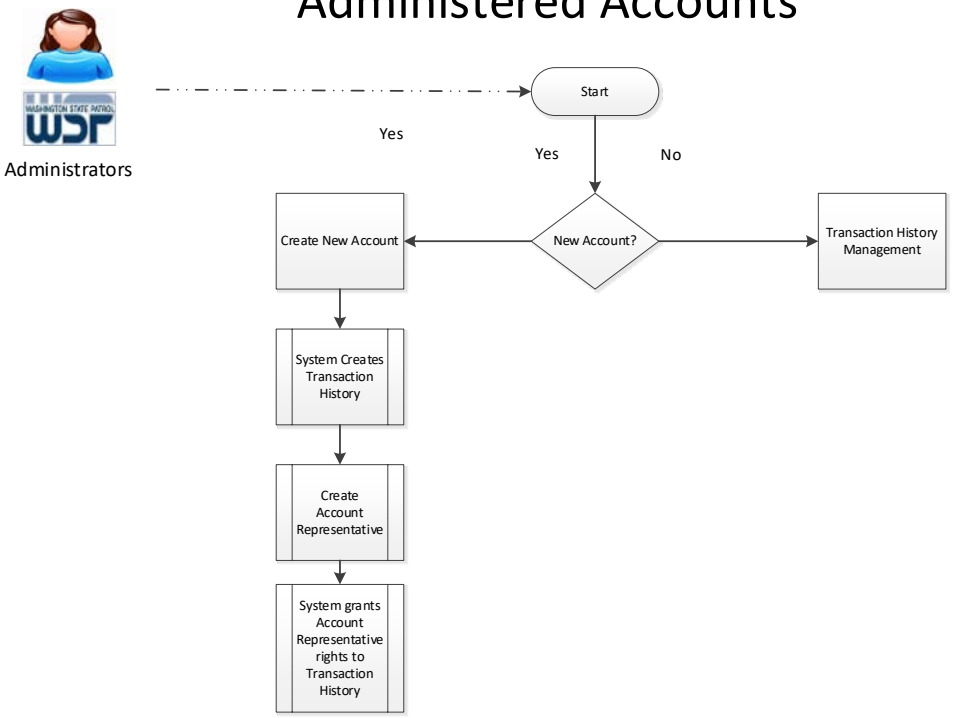
Event Description
Public user creates an account and system creates the transaction history. System makes the user the Account Representative which grants them full rights to the transaction history
Public user accesses transaction history. As Account Representative they own and maintain the transaction history and all items in transaction history
The WSP Administrator creates an Administered Account and system creates the transaction history. As WSP Administrator they have access to all items in transaction history
The WSP Administrator assigns Account Representatives to account. As Account Representative they own and maintain the transaction history and all items in transaction history.
The Account Representative accesses the transaction history. They view, print, download or delete items
The WSP Administrator or Account Representative creates users and assigns account roles to them.
The system moves items from the inbox to an archive using parameters set by the WSP Administrator.
Account User accesses the transaction history and the system limits the items available based on account role
The system monitors the contents of the transaction history (inbox & archives) and sends notification to Account Representative when transaction history is almost full.

Event Description
The system monitors the contents of the transaction history and sends notification to Account Representative that transaction history is full. The system prevents anymore items from being added to the transaction history until space is made.

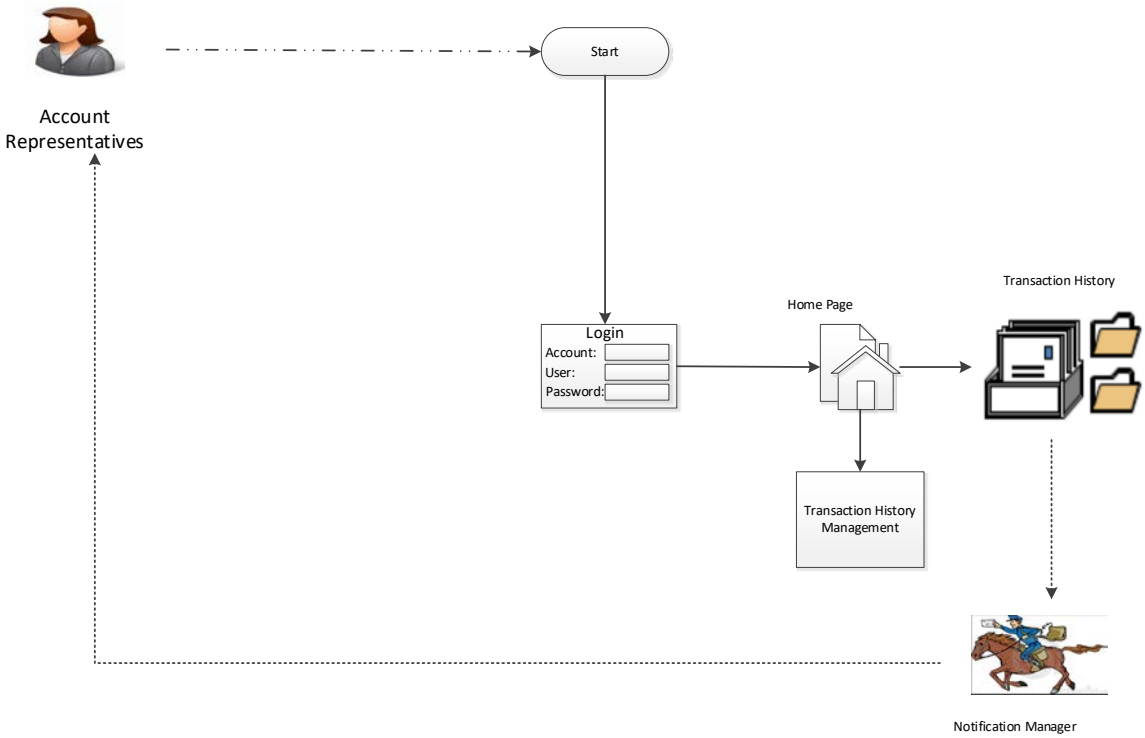
1.13.4 Process Steps

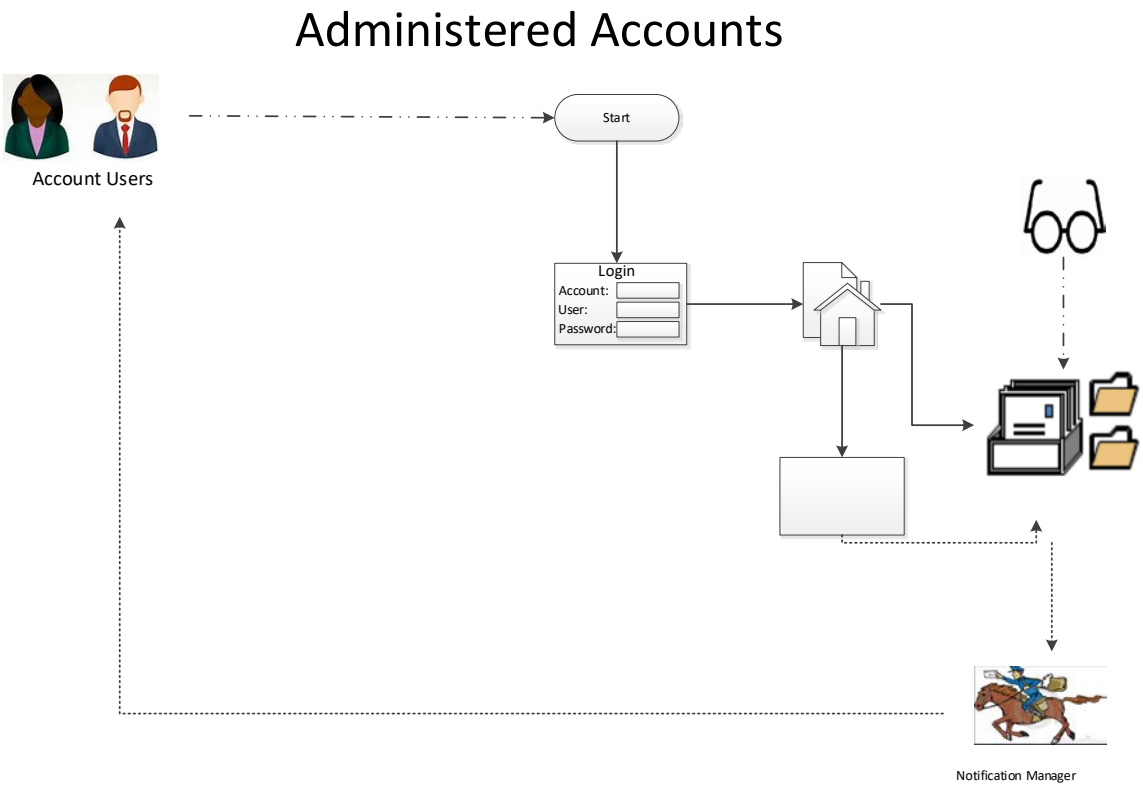


Administered Accounts



Administered Accounts





1.13.5 Functional Requirements

Ref #	Requirement	Priority
THM 01	For each account created the system will create a transaction history comprised of an inbox and an archive	Mandatory
THM 02	The system will recognize Account Representatives as the owners of their transaction histories and grant them full access to all items in the transaction history and grant them full authority to manage the contents of their transaction history.	Mandatory
THM 03	The system grants the WSP Administrator full authority to all transaction histories	Mandatory
THM 04	The system will control access to transaction histories and the items in a transaction history based on Account Role assigned to an Account User.	Mandatory
THM 05	The system must have a process to move items from the inbox to the archive using parameters set by the WSP Administrator.	Mandatory
THM 06	The system must notify Account Representatives when their transaction history is almost full.	Mandatory

Ref #	Requirement	Priority
THM 07	The system must notify Account Representatives when their transaction history is full and cannot accept any more items.	Mandatory
THM 08	The system must prevent items being added to the transaction history when it has reached it maximum storage capacity.	Mandatory
THM 09	CRD Staff must be able to easily lookup and audit all transaction history maintenance. The lookup must offer a variety of search criteria.	
THM 10	The system must log all transaction history maintenance actions including the date/time, user id, account, IP address, action (deleted items, down loaded items.)	Mandatory

1.14 Message Management (S)

Every CRD customer must have a web portal account. Each account has a message queue. There are two types of accounts:

Public – Create and maintain their accounts. Public users manages their message queue.

Administered Accounts – The Account Representative manages the message queue and assigns access to account users.

The work processes documented within Message Services Management include:

- Create Message Queue
- Access Message Queue
- Create a Message
- Read a Message
- Reply to Message
- Forward a Message
- Delete a Message
- Clear a Message Queue
- Send Notification of New Message

Business Process Detail Description

1.14.1 Process Description

The system creates a message queue for an account when the account is created. The message queue is a means of asynchronous communication between the account and CRD. It provides WSP and its customers with a secure method to communicate sensitive information. It is not intended for synchronous real time chats between users and WSP staff. Support on the web portal is expected to be provided by a Chatbot, FAQs and Context Sensitive Help (CSH).Users access their messages from their home page. The user can create a message or reply to a message sent from the system or CRD. The system routes the message to the appropriate CRD message queue. CRD staff can send messages or respond to messages. The Account Representative maintains the queue and can delete messages. The system runs a regular clean-up program that deletes old messages (based on variable parameters) from message queues. The user may elect to receive notification when a new messages arrives in their queue by using Notification Services. The system will trigger the notification as part of the message delivery.

1.14.2 Actor / System

Actor	Goal
Public User	Reads messages in their message queue, creates messages, replies to messages and deletes messages. Uses notification services to receive notifications when messages are delivered.
WSP Administrator	Sets up and maintains the Account Representative. Accesses messages routed to the Administrator queue.

Account Representative	Manages access to message queue. Can delete messages in queue. Can grant account roles rights to create forward and delete messages.
Account User	Accesses the message queues from their home page. Account users have default read and respond access to messages based on account roles. Can be granted authority to create, forward and delete messages.

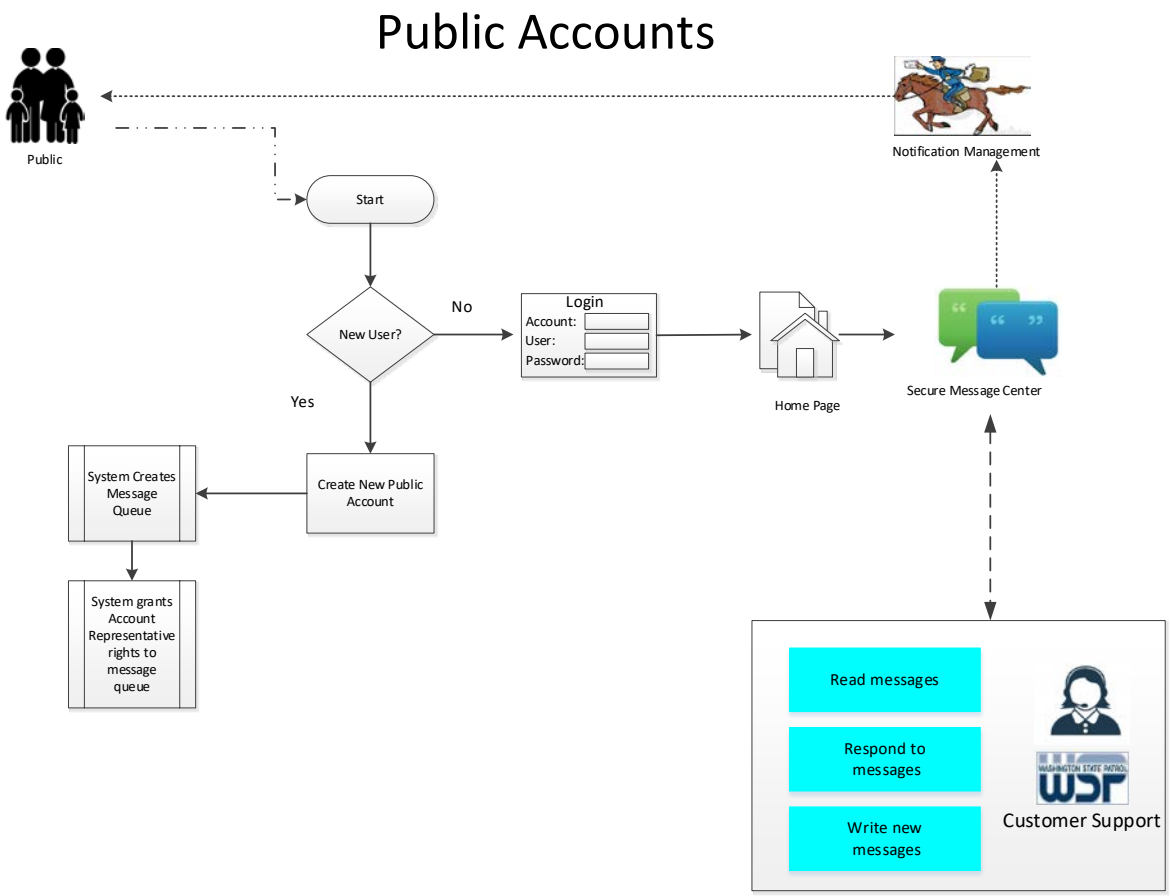
System	Purpose
The System	• Creates and assigns a message queue when the account is created. • Publishes a visual alert on the home page to notify the user that they have new messages. • May trigger notifications services when new messages are delivered. • Routes account messages to appropriate CRD queue based on message request. • Routes CRD messages to account message queue. • Purges messages based on criteria provided. • Uses role based security to manage access to messages.

1.14.3 Triggering Events

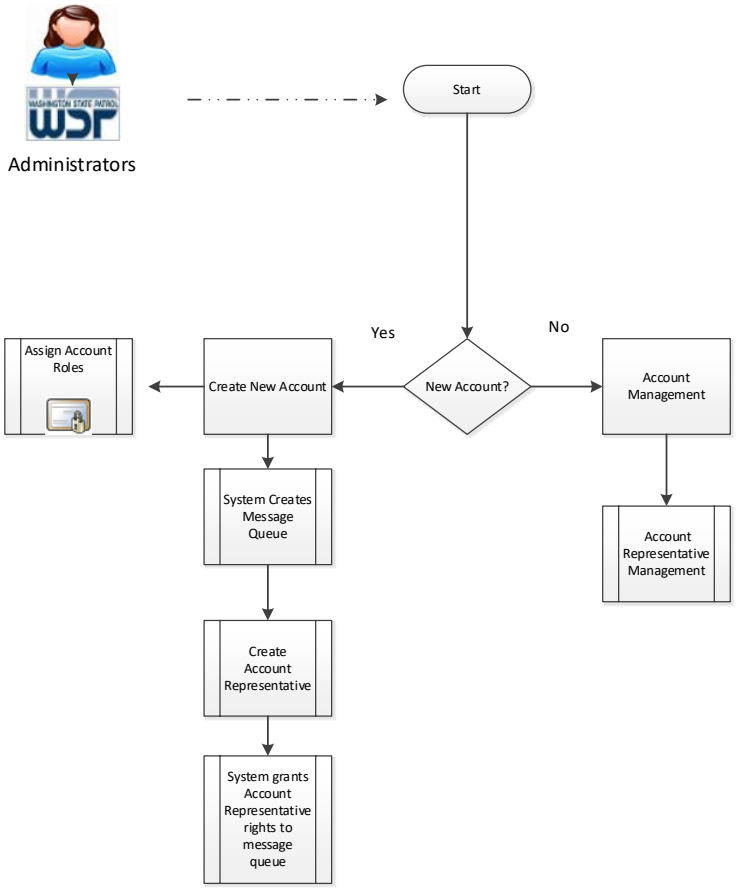
Event Description
As part of establishing a new Account, the system creates a message queue for the account and assigns the Account Representative rights to the queue.
Account Roles are used to determine where messages are routed at WSP.
A user logs into the portal and navigates from their home page to their message center to read messages and respond to in their queue
The user reads, creates or replies to messages
The system routes messages to appropriate message queue based on the Account Role of the sender
CRD staff access messages routed to their queue
CRD staff read, reply, forward and create new messages. The system routes these messages to the appropriate message queue.

Event Description
The system generates and sends preformatted messages to the user's message queue in response to regular events occurring. (**examples**: "your password will expire in 30 days" "A credit has been posted to your account")
An Account Representative deletes messages from their queue
The system will regularly purge old messages from message queues after a proscribed length of time.
The system generates and sends preformatted messages to the user's message queue in response to regular events occurring. (**examples**: "your password will expire in 30 days" "A credit has been posted to your account")
The system will notify users when a new message is delivered to their queue if their notification services are configured to do so

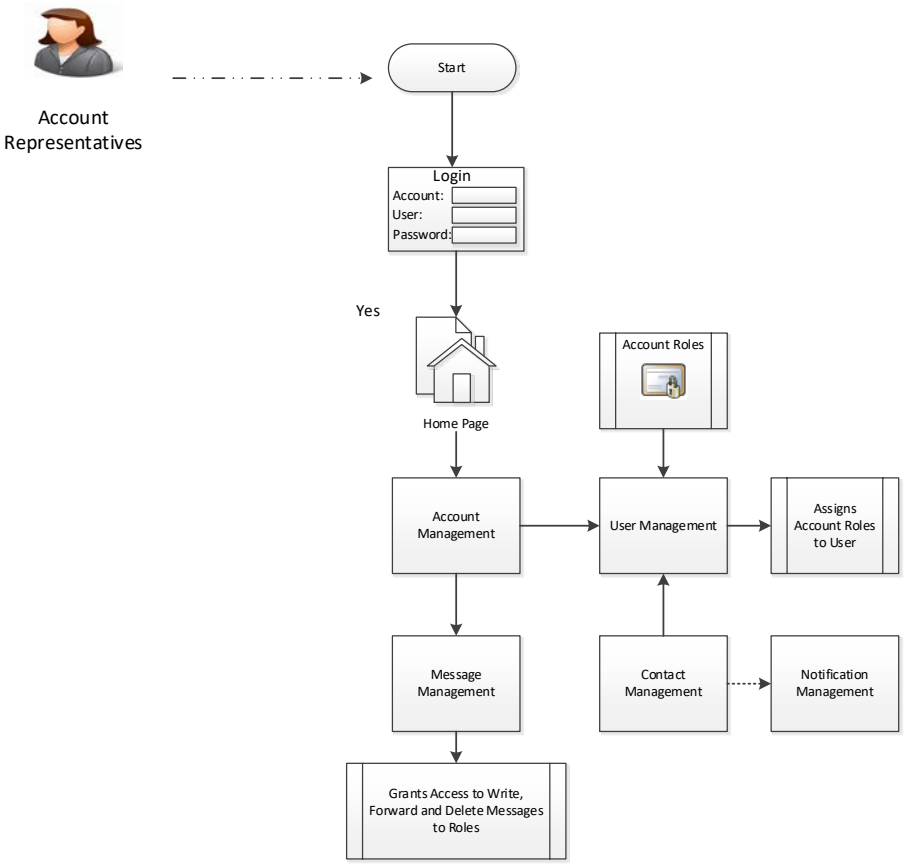
1.14.4 Process Steps



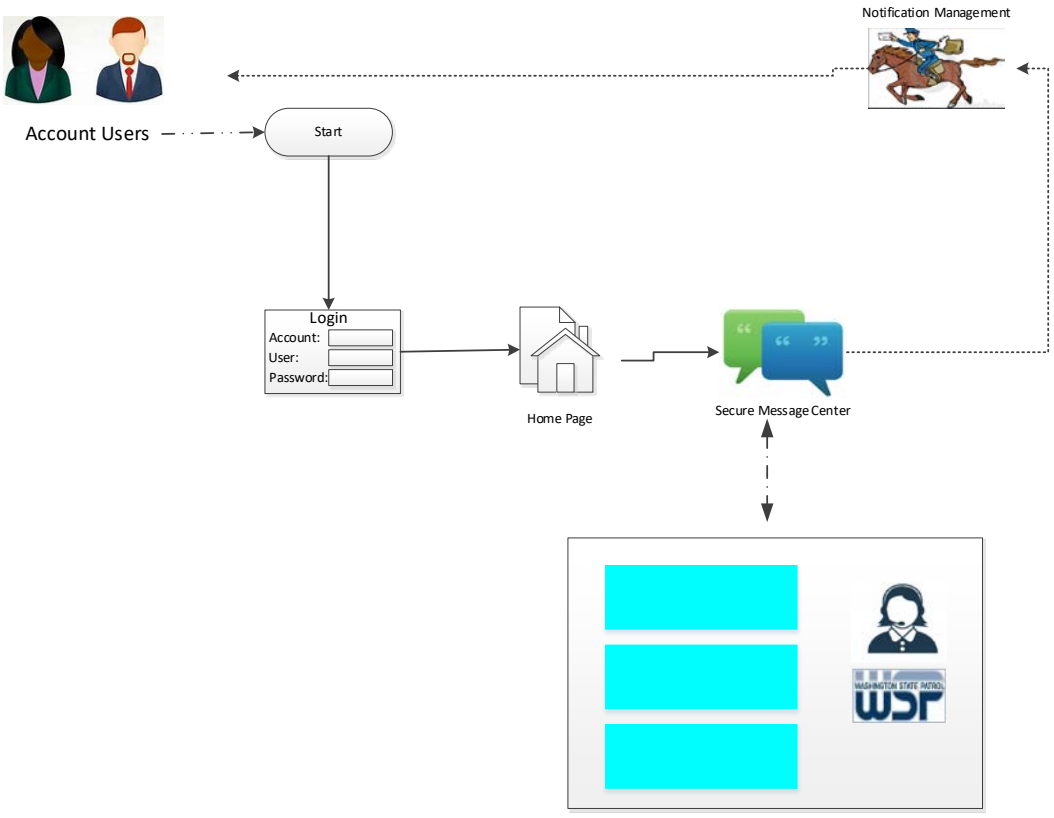
Administered Accounts



Administered Accounts



Administered Accounts



1.14.5 Functional Requirements

Ref #	Requirement	Priority
MSM 01	Each account will have a message queue	Mandatory
MSM 02	Each account can access its message queue from its homepage	Mandatory
MSM 03	Access to messages is based on the Account Role assigned to a user	Mandatory
MSM 04	Each user can read their messages	Mandatory
MSM 05	Each user can reply to their messages	Mandatory
MSM 06	Each user can create messages and send them	
MSM 07	The Account Representatives can read all messages for the Account	Mandatory
MSM 08	The Account Representatives can reply to all messages for the Account	Mandatory

Ref #	Requirement	Priority
MSM 09	The Account Representatives can delete messages in their message queue	Mandatory
MSM 10	WSP Administrators and CRD staff can create messages and send them to users	Mandatory
MSM 11	WSP Administrators and CRD staff can read messages from users	Mandatory
MSM 12	WSP Administrators and CRD staff can reply to messages from user	Mandatory
MSM 13	WSP Administrators and CRD staff can forward messages to other CRD staff	Mandatory
MSM 14	CRD Staff must be able to easily lookup and audit all messages. The lookup must offer a variety of search criteria.	Mandatory
MSM 15	The system must log all message queue activities including the date/time, user id, account, IP address, action (create, send, delete, reply)	Mandatory

1.15 Notification Management (S)

Every CRD customer must have a web portal account. There are two types of accounts:

Public – Create and maintain their accounts. They create and manage their notification requests.

Administered Accounts – The WSP Administrator creates and maintains the account. The Account Representative creates and manages notification requests for Account Roles.

The work processes documented within Notification Management include:

- Create a Notification Request
- Manage a Notification Request
- Delete a Notification Request
- Schedule a Notification Request
- Create a Notification
- Send Notification

Business Process Detail Description

1.15.1 Process Description

Each account can request Notifications. A notification is an email or text message sent when an event occurs. This message contains no sensitive information, it is simply a notification that some event or action has occurred that the user has requested to be notified when it occurs. The Notification Service allows the account to associate the event with the role being notified. The address information and notification preference (email, text message) are maintained at the role level in Contact Management. Notification Management defines the conditions that generate a notification. For example, a role requests to receive an immediate notification when a new message is delivered into their message queue. The system sends the notification when it delivers the message. Notifications themselves are highly generic, system generated messages that inform the user as to the reason they should access the portal. They do not include confidential information nor require encryption. Account Representatives can request, modify and delete notifications. The WSP Administrator can request and schedule system wide notifications for events such as system outages. When events occur the system uses notification services to process notifications.

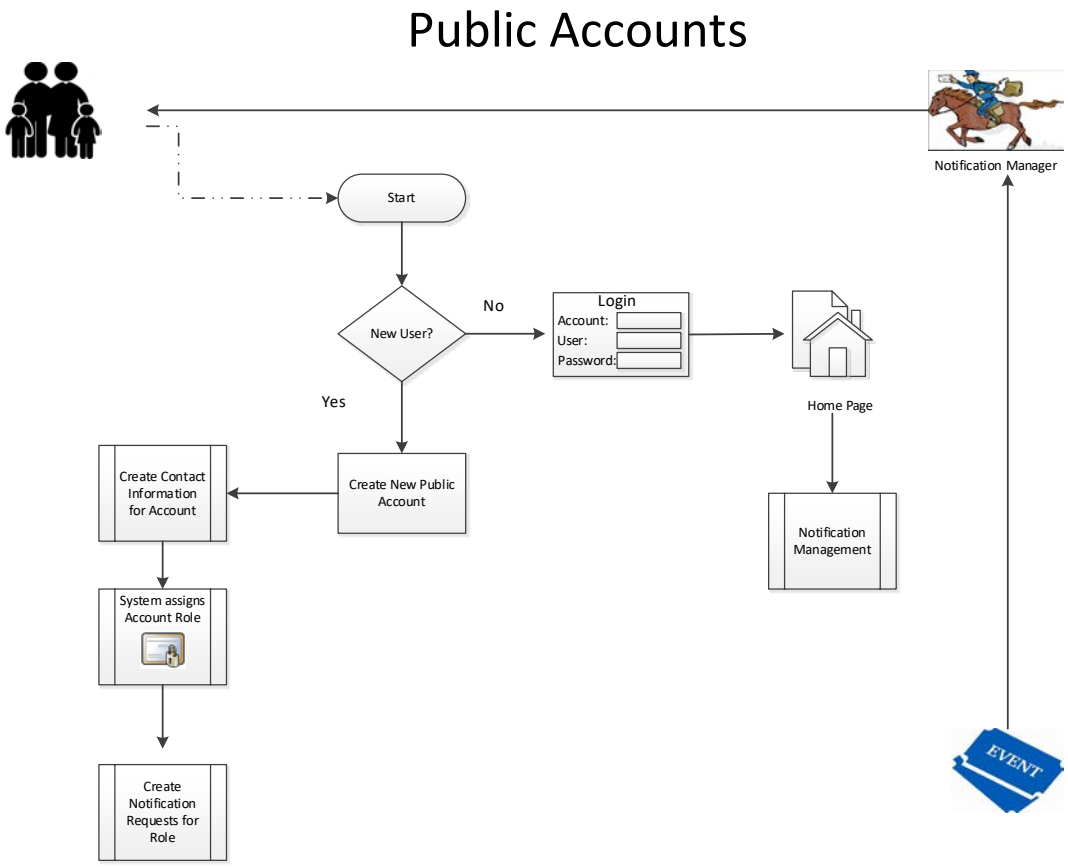
1.15.2 Actor / System

Actor	Goal
Public User	Requests and maintains notifications. Receives notifications.
WSP Administrator	Creates and schedules system wide notifications
Account Representative	Requests and maintains notifications for Account Roles assigned to Account.
Account User	Receives notifications based on account role assigned
System	**Purpose**
The System	Enforces the rules for Notification Management. Generates Notifications based on requests in Notification Management.

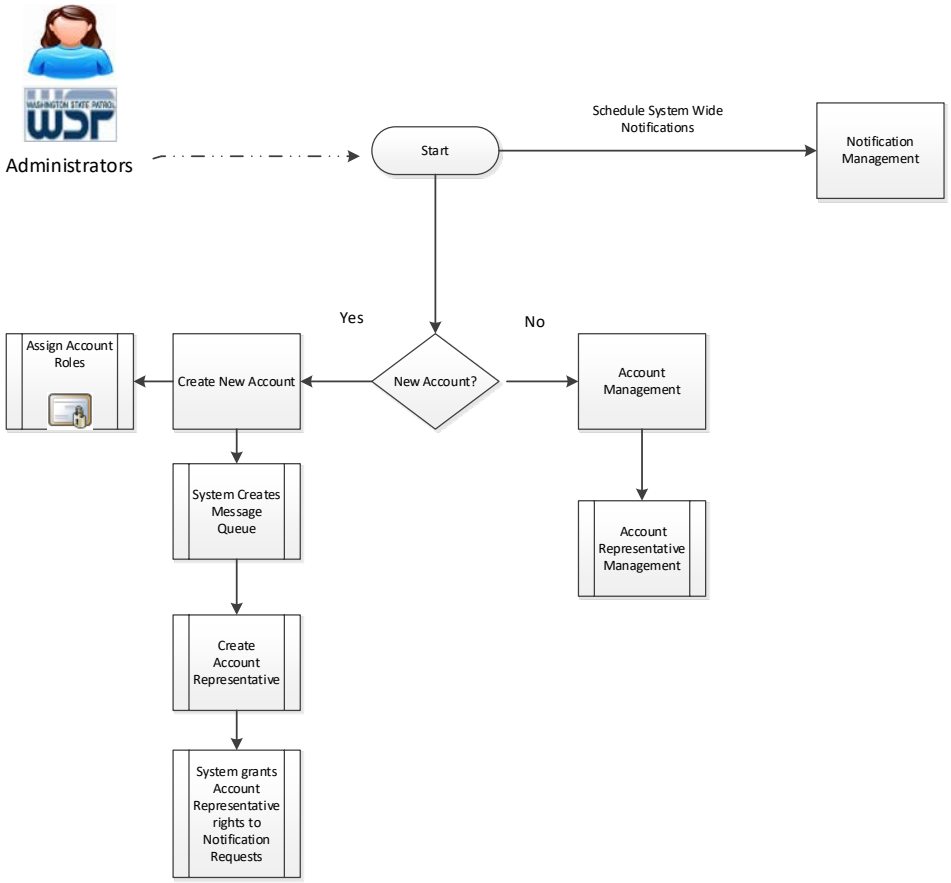
1.15.3 Triggering Events

Event Description
A Public User receives a notification
Account User receives a notification
Account Representative requests a notification for an event and associates an Account Role
Account Representative modifies a notification request
Account Representative deletes a notification request
WSP Administrator requests a system wide notification
The System uses the addresses in Contact Management to send notifications
The System generates the text and sends a notification

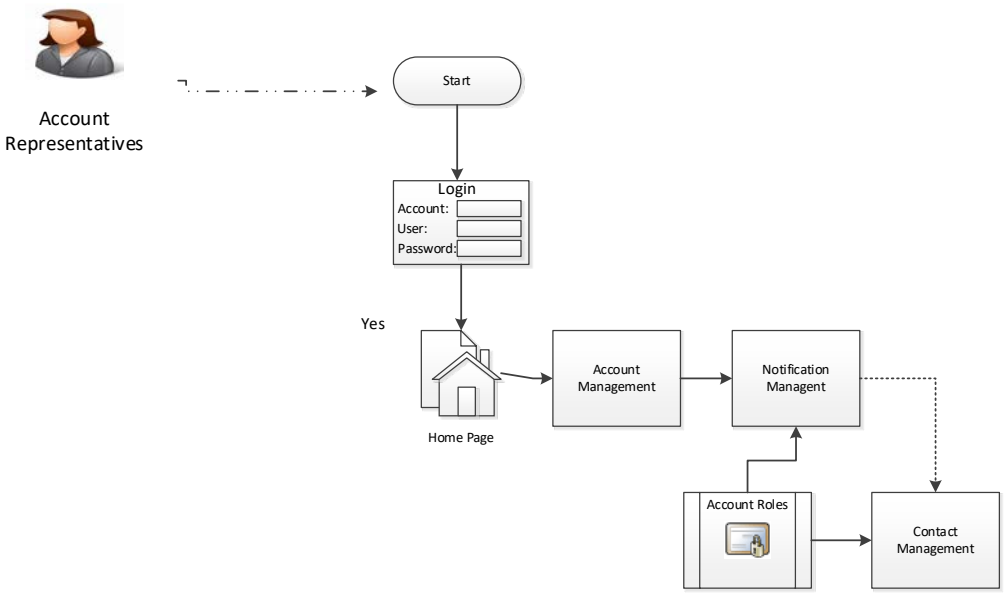
1.15.4 Process Steps



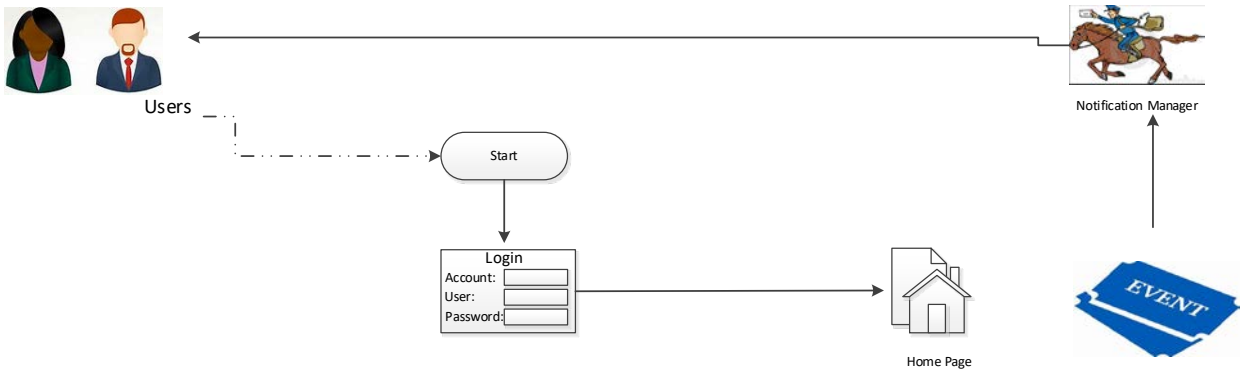
Administered Accounts



Administered Accounts



Administered Accounts



1.15.5 Functional Requirements

Ref #	Requirement	Priority
NOM 01	The system must have a list of triggering events (new message, new item in transaction history, etc.) that can be associated with roles to create notification requests.	Mandatory
NOM 02	The system must enforce that only authorized roles are associated with triggering events.	Mandatory
NOM 03	If a role is no longer authorized then its associations with events are deleted.	Mandatory
NOM 04	The system must have a list of maintainable generic messages that are associated with triggering events.	Mandatory
NOM 05	The system must supply a maintenance tool to maintain generic messages and set their association with triggering events.	Mandatory
NOM 06	The system must generate messages using generic messages and the associated triggering event.	Mandatory
NOM 07	The system must send notifications to the addresses for the associated roles.	Mandatory
NOM 08	The system must monitor for event occurrences and retain the information until a scheduled time when notifications are generated and delivered	Mandatory
NOM 09	Account Representatives must be able to associate events and roles to create Notification Requests	Mandatory
NOM 10	WSP Administrators must be able to create and schedule system wide notifications	Mandatory

Ref #	Requirement	Priority
NOM 11	CRD Staff must be able to easily lookup and locate notification requests for Administered Accounts. The lookup must offer a variety of search criteria.	Mandatory
NOM 12	The system must log all notification management actions including the date/time, user id, account, IP address, action (establish account, change account, disable account, enable account, delete account)	Mandatory

1.16 Criminal History Request – NDOB (S)

A primary purpose of the web portal is to perform Name, Date of Birth (NDOB) background checks for a fee. The Web Portal requests the background check search through an API with WASIS. The background check is performed by WASIS and the search results are returned to the Web Portal and posted in the Transaction History. The user enters a first name, last name, middle initial, a date of birth up to 9 other names used and an optional gender. The web portal submits the search to WASIS and the search results (either a rapsheet or a statement that the person has no criminal record) are returned to the Web Portal to be posted in the transaction history. There are two types of web portal accounts:

Public Accounts – Users in public accounts request NDOB background checks. They pre-pay via credit card and are charged a fee per search.

Administered Accounts – Users in Administered Accounts may request NDOB background checks if they are permitted by the account roles assigned to them. "Billed" accounts are charged a fee per search and the account is invoiced on a monthly basis. "Non-Billed" accounts are not charged for the service.

The work processes documented within NDOB Background Check Services include:

- Request a NDOB Background Check
- Charge for a NDOB Background Check
- Retrieve a Background Check Result

Business Process Detail Description

1.16.1 Process Description

1.16.2 Actor / System

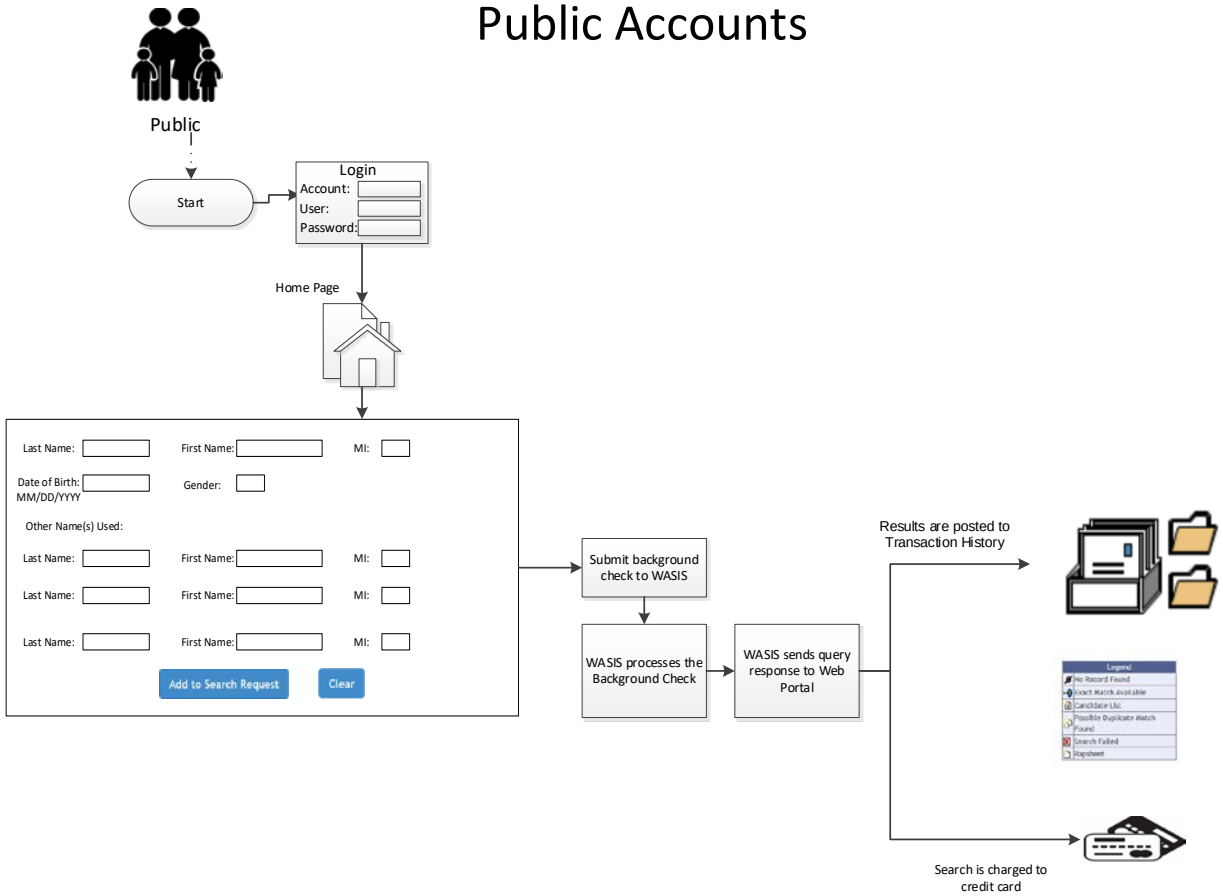
Actor	Goal
Public User	Enters a combination of name and date of birth, up to 9 other names used and submits a request for background check. The search is processed by WASIS. The results will be posted to their transaction history where the user can retrieve the results from the transaction history. The user's credit card is charged for the service.
Account User	Enters a combination of name and date of birth, up to 9 other names used and submits a request for a background check. The search is processed by WASIS. The results will be posted to their transaction history where the user can retrieve the results. The web portal transmits the charge activity to WASIS.
System	**Purpose**

System	Enforces the rules for NBOD Background Checks. Processes the background checks and publishes the results in the Account transaction history.

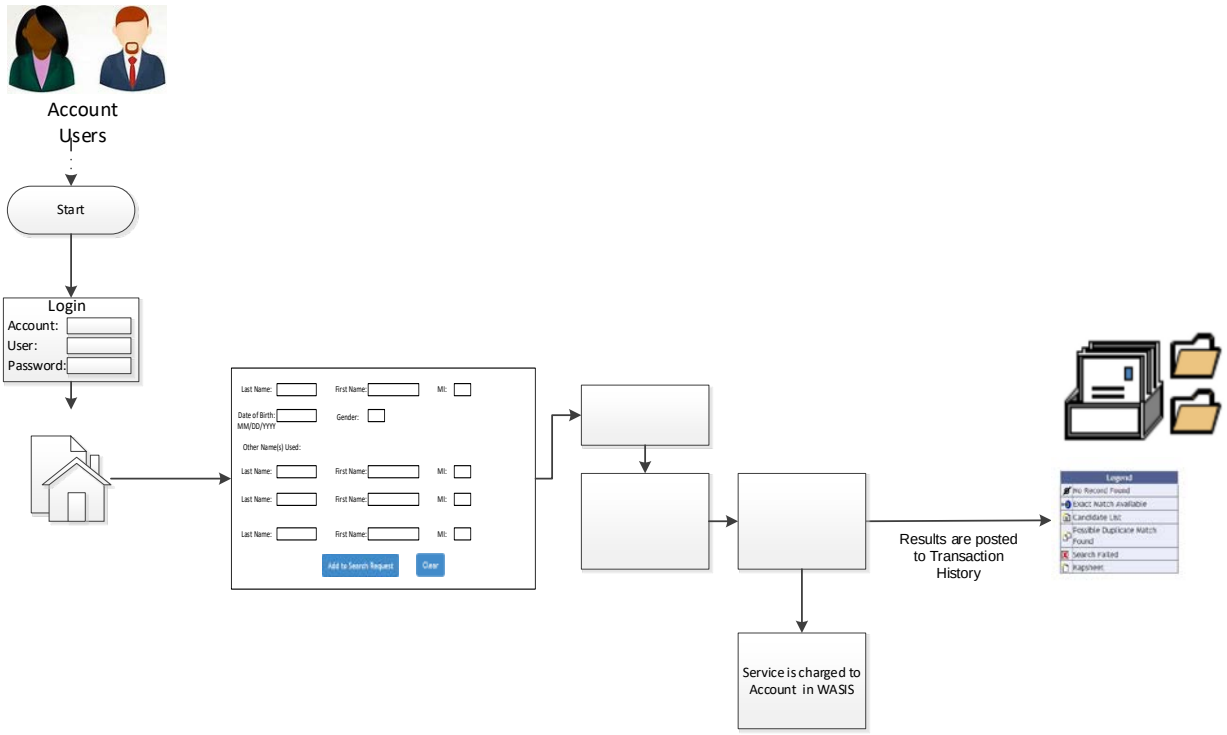
1.16.3 Triggering Events

Event Description
Public User requests a NDOB Background Check
An Account User requests a NDOB Background Check

1.16.4 Process Steps



Administered Accounts



1.16.5 Functional Requirements

Ref #	Requirement	Priority
NBC 01	Users must be able to enter a name for the subject	Mandatory
NBC 02	Users must be able to enter up to 9 other names used	
NBC 03	Users must enter a valid date of birth	Mandatory
NBC 04	The system must validate the date of birth entered	Mandatory
NBC 05	The user must enter at least one last name	Mandatory
NBC 06	The system must validate the last names entered	Mandatory
NBC 07	The user must enter at least one character for a first name	Mandatory
NBC 08	The user may enter a middle initial for each subject entered	Mandatory
NBC 09	The user may select a gender for the subject	Mandatory
NBC10	The system passes the search request to WASIS via an API	Mandatory
NBC 11	The system passes charges to third party credit card interface for public account NDOB searches	Mandatory
NBC 12	The system retrieves the search result via an API and posts to the results to transaction history	Mandatory

Ref #	Requirement	Priority
NBC 13	CRD Staff must be able to easily lookup and audit all NDOB searches. The lookup must offer a variety of search criteria.	Mandatory
NBC 14	The system must log all NDOB Searches including the date/time, user id, account, IP address, action (search criteria)	Mandatory

1.17 Criminal History Request – Unique Identifier (S)

A Criminal Justice Administered Account has a user who has information returned on a previous criminal history search may request a rapsheet for candidates by either SID or FBI#. Both of these numbers are unique numbers in WASIS. When the user enters a unique identifier for this candidate the system will only search for an exact match. The user submits the search to WASIS and WASIS performs the search. The search results (a rapsheet) or a message that there was no exact match is returned to the system. The system posts the search results in their transaction history. When the WSP Administrator sets ups an Administered Account they identify if that account is a Criminal Justice Account (see Appendix B – Interface Types).There are two types of web portal accounts:

Public Accounts – Have no access to background checks by unique identifiers.

Administered Accounts – Only users in Administered Accounts that are authorized (Criminal Justice accounts) may request background checks by unique identifiers if they are permitted by the account roles assigned to them. **Note** (WASIS Service): "Billed" accounts are charged a fee per search and the account is invoiced on a monthly basis. "Non-Billed" accounts are not charged for the service.

The work processes documented within Background Check by Unique Identifier include:

- Request a Background Check by Unique Identifier
- Route the results of a search by unique identifier to the transaction history
- Charge the user's account for a Background Check search
- Retrieve a Background Check search result from the transaction history

Business Process Detail Description

1.17.1 Process Description

1.17.2 Actor / System

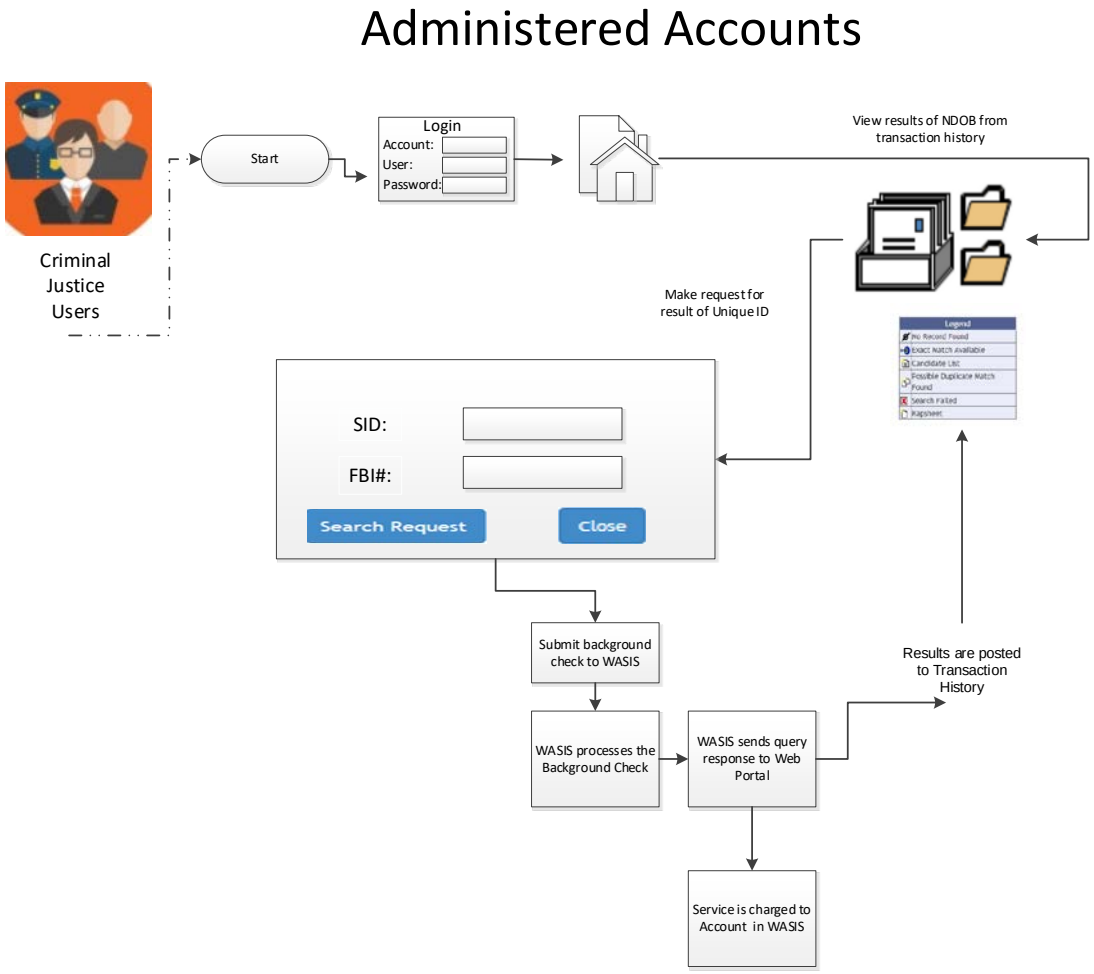
Actor	Goal
Account User (Criminal Justice Accounts only)	Enters a unique identifier and requests a background check. The results will be sent to their transaction history where the user can retrieve the results from the transaction history. If this is a billed account the account is charged for the search. If this is a non-billed account is not charged.
System	**Purpose**

System	Enforces the rules for Background Checks by unique identifier. Processes the background checks and publishes the results in the Account transaction history.

1.17.3 Triggering Events

Event Description
An Account User requests a Background Check by unique identifier

1.17.4 Process Steps



1.17.5 Functional Requirements

Ref #	Requirement	Priority
UIM 01	User must enter a unique ID (SID or FBI#) that meets the field edits for the IDs	Mandatory

Ref #	Requirement	Priority
UIM 02	The system uses an API with WASIS to confirm that there is a record for the unique id entered	Mandatory
UIM 03	The system passes the search request to WASIS via an API	Mandatory
UIM 04	The system retrieves the search result via an API and posts to the results to transaction history	Mandatory
UIM 05	The system must route a notification to the user that the result is in their transaction history if they have notification services configured.	Mandatory
UIM 06	CRD Staff must be able to easily lookup and audit all unique identifier requests. The lookup must offer a variety of search criteria.	Mandatory
UIM 07	The system must log all unique identifier requests including the date/time, user id, account, IP address, action (search criteria)	Mandatory

1.18 Notary Services Management (S)

Every CRD customer must have a web portal account. There are two types of accounts:

Public – Create and maintain their accounts. A public user may request notarized letters. Through contact management a user establishes their preferred method of delivery for notarized letters and can either use that method or provide an alternative when they make their request.

Administered Accounts – Account users may request notarized letters. Through contact management a user establishes their preferred method of delivery for notarized letters and can either use that method or provide an alternative when they make their request.

The work processes documented within Notary Services Management include:

- Configure Notary Services for an Account
- Request Notarized Letter
- Request Special Handling
- Process a Notarization Request
- Send Notification that a Notification Request has been processed

Business Process Detail Description

1.18.1 Process Description

Accounts can request a notarized letter verifying that they have no criminal history. For the public these documents are pre-paid by credit card. The system logs the request and routes it to BGU staff to process. The user may request special handling to expedite the process. The system uses message management to send status messages to the requestor and sends a notification to the user. Contact information for user is used for mailing address for items.

Users of Administered Accounts can request notary letters. The cost of these requests is charged to their account. The system logs the request and route it to BGU staff who process the request. Contact information for the Account Role is used for mailing address for items.

The Administrator can revoke the authority to request notary services to any customer.

1.18.2 Actor / System

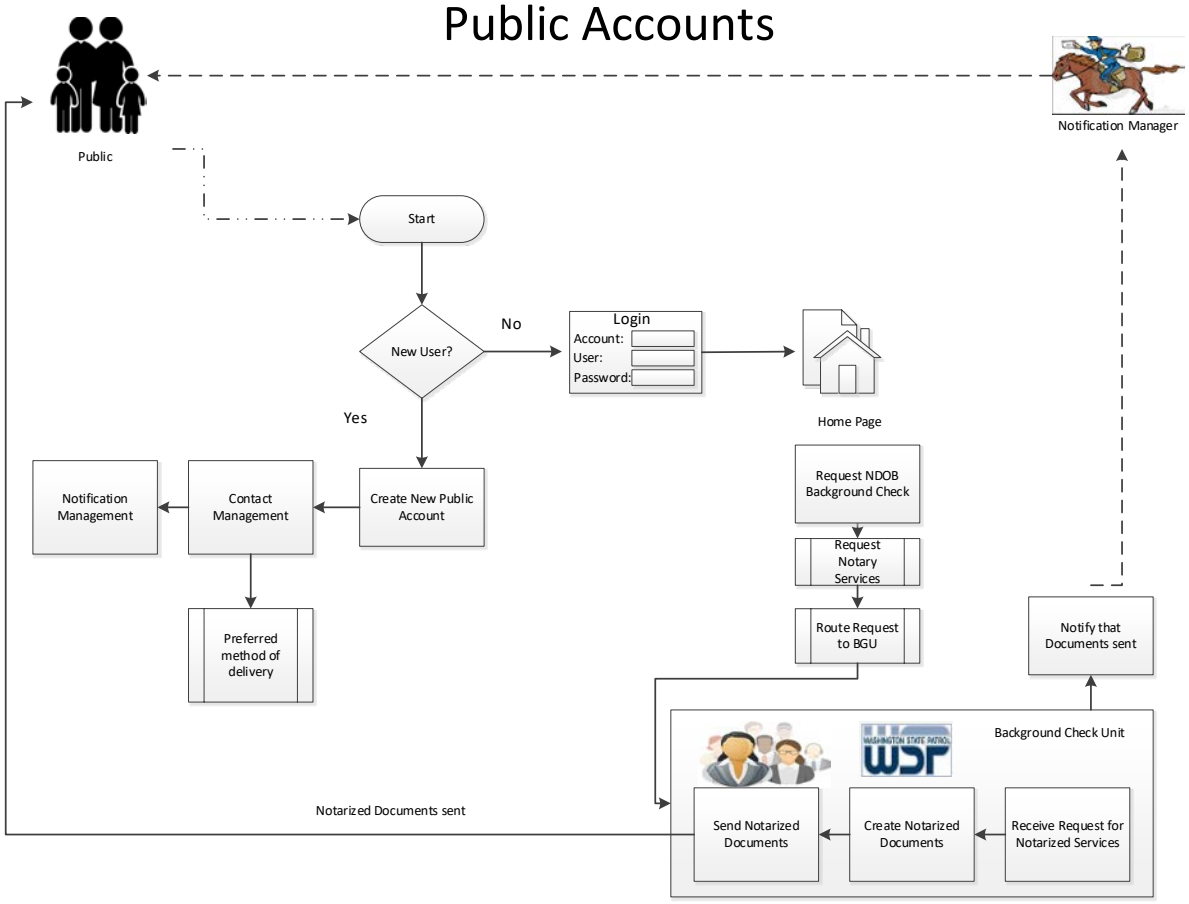
Actor	Goal
Public User	Request notarized copies or notarized letters.
WSP Administrator	Grants authority to Administered Accounts. Can revoke the authority for any account.
Account Representatives	N/A
Account User	Request notarized letters.

BGU Staff	Receive requests for Notary Services. Processes the request and sends the response via postal service. Runs reports that list all notary service requests and their current status.
System	**Purpose**
The System	Processes requests for notary services. Fees are charged and public users are reminded that their credit card will be charged for the services. Administered Accounts are charged and are either invoiced or not based on payment type.

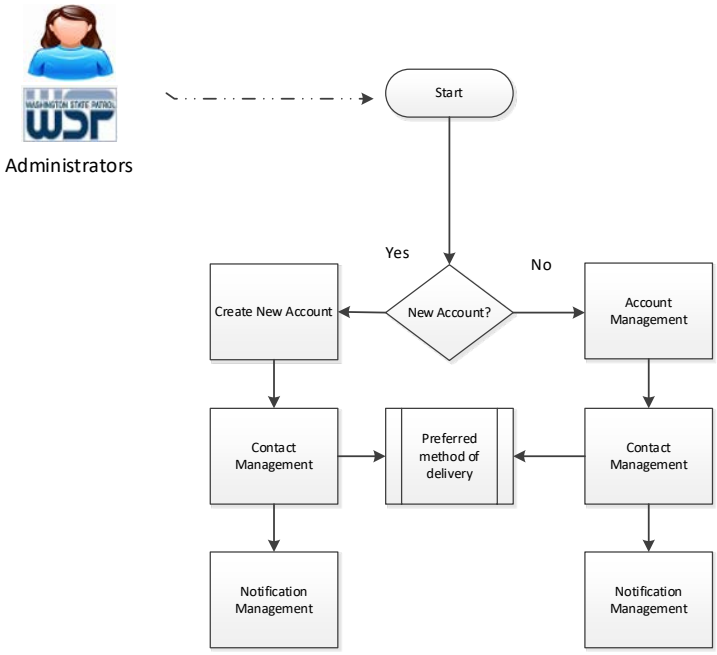
1.18.3 Triggering Events

Event Description
After running a criminal history search a user requests a notary letter
The WSP Administrator in setting up an administered account grant's the customer notary services
The WSP Administrator revokes access to notary services for a customer
The system receives a request for notary services from a customer and routes the information to BGU work queue
BGU staff will process notary requests and update the status of the request
The system notifies the customer of the changing status of their notary request as it is processed by BGU.
BGU staff run reports that list notary services requests and their status

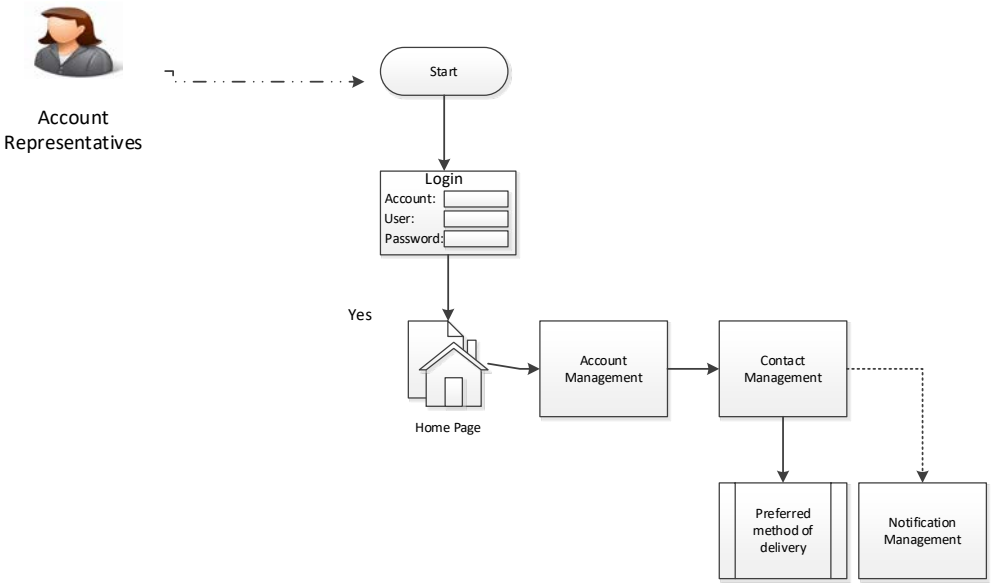
1.18.4 Process Steps



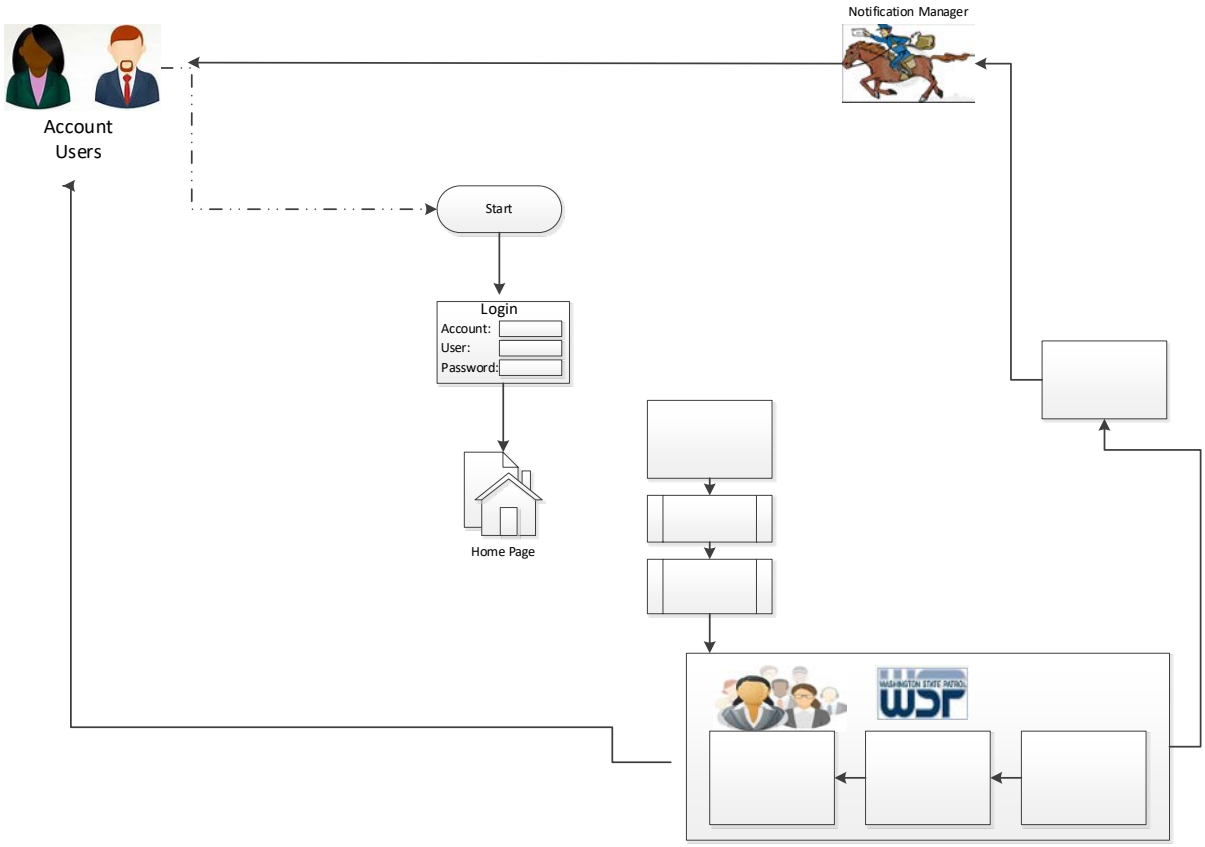
Administered Accounts



Administered Accounts



Administered Accounts



1.18.5 Functional Requirements

Ref #	Requirement	Priority
NSM 01	The system will automatically grant authority for notary services to any public account when it is established	Mandatory
NSM 02	Administrators can grant authority for notary services to any Administered Account	Mandatory
NSM 03	Administrators can revoke authority for notary services for any account	Mandatory
NSM 04	Any users can request notary services for background checks that have been processed and reside in their transaction history.	Mandatory
NSM 05	Administrators can set limits on how old the transactions are that can qualify for Notary Services.	Mandatory
NSM 06	The system will validate the request for Notary Services from the customer	Mandatory

Ref #	Requirement	Priority
NSM 07	The system will charge the credit card of Public Users for Notary Services	Mandatory
NSM 08	The system will charge the Administered Account for Notary Services	Mandatory
NSM 09	The system will route requests for Notary Services to a BGU work queue	Mandatory
NSM 10	The system will notify BGU staff that when requests are routed to their work queue	Mandatory
NSM 11	The system will support BGU staff posting updated statuses for the processing of notary requests	Mandatory
NSM 12	The system will route notary request status information to the customer via notification and message services	Mandatory
NSM 13	The system must prompt users as to whether the address located in contact information is the address the notary copies or letter will be sent to	Mandatory
NSM 14	BGU Staff must be able to easily lookup and locate the status of Notary Request. The lookup must offer a variety of search criteria.	Mandatory
NSM 15	The system must log all account actions including the date/time, user id, account, IP address, action (request notary copies, request notary letter)	Mandatory

1.19 Subscription Management (S)

The Subscription services are a new service intended to be offered to select Web Portal customers. The only two subscription services currently under consideration are a subscription to receive ABIS messages as emails instead of text messages and Rapback services. Every CRD customer must have a web portal account. There are two types of accounts:

Public - Create and maintain their accounts. Public users are not offered any subscription services.

Administered Accounts – The WSP Administrator creates and maintains the account. These accounts can offered subscriptions services if they meet the qualifications of the agency. The Account Representatives create and maintain Subscriptions. Subscription data is sent to the account transaction history and a notification is sent to the Subscriber.

The work processes documented within Subscription Management include:

- Grant Subscription Services for an Account
- Maintain Subscription Services for an Account
- Revoke Subscription Services for an Account
- Subscribe
- Maintain Subscription
- Delete Subscription
- Send Notification of Subscription Event
- Deliver Subscription Data

Business Process Detail Description

1.19.1 Process Description

When the WSP Administrator creates an Administered Account they may grant the account access to subscription services. The WSP Administrator can grant these services at a later date, change the terms of the services granted, or revoke those services. Subscription services is the association of the subscription event with an Account Role. Notifications of subscription events are managed through the Notification Services. The only subscription services currently planned to be offered are receiving ABIS messages as emails and Rapback. The Account Representative will fill in the subscription to subscribe to the service and in the case of rapback, users assigned the subscription (by role) can identify the persons for whom rapback is requested for. The system enforces the rules for subscription services. Subscriptions are not offered to public users. Rapback subscriptions are only offered to Criminal Justice (CJ) customers.

1.19.2 Actor / System

Actor	Goal
Public User	N/A
WSP Administrator	Grants, maintains, and revokes subscription services for an administered account that qualifies
Account Representative	Subscribes a role to request rapback services or ABIS messages

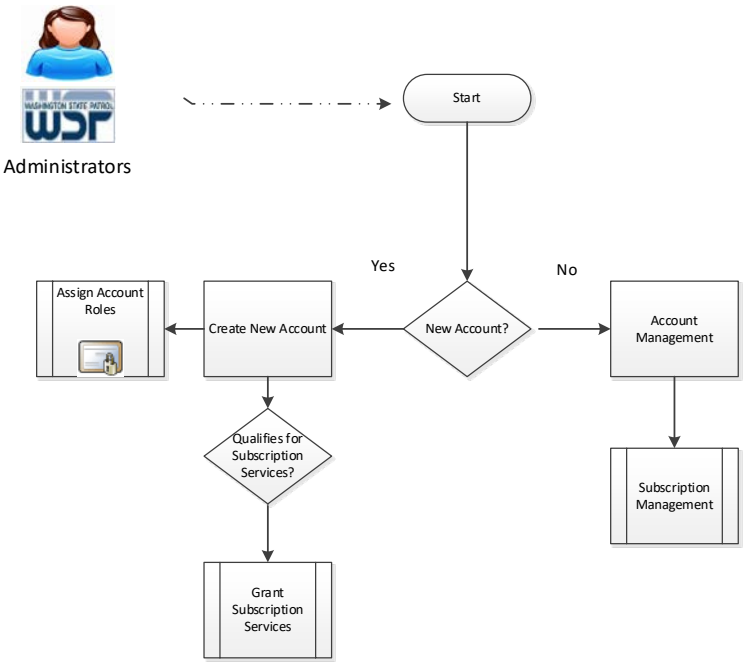
Account User (ABIS Coordinator)	Requests ABIS messages as emails
Account User (Criminal Justice Accounts only)	Request rapback services for persons
System	**Purpose**
The System	Enforces the rules for subscription services

1.19.3 Triggering Events

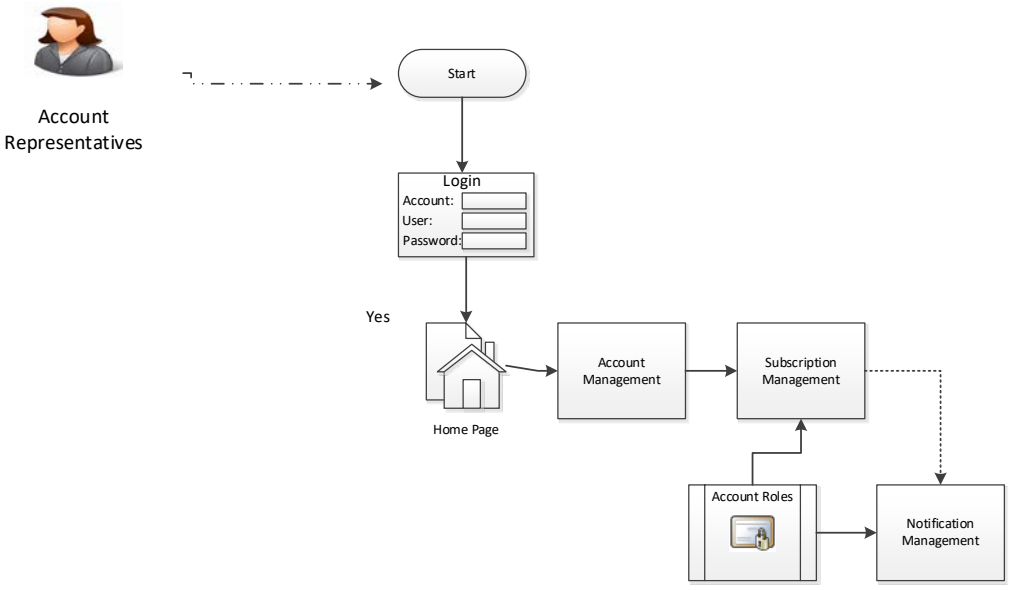
Event Description
The WSP Administrator creates the account and grants subscription services
The WSP Administrator updates the account and grants subscription services
The WSP Administrator updates the account and revokes subscription services
The Account Representative subscribes a role to a subscription service
The Account Representative unsubscribes a role to subscription service
A user with a subscribed role requests rapback services for persons.
A user with a subscribed roles requests email ABIS messages
The system sends the user request to WASIS via an API
A subscription triggering event occurs, the subscribed product may be delivered to the account transaction history and a notification is sent to the role.

1.19.4 Process Steps

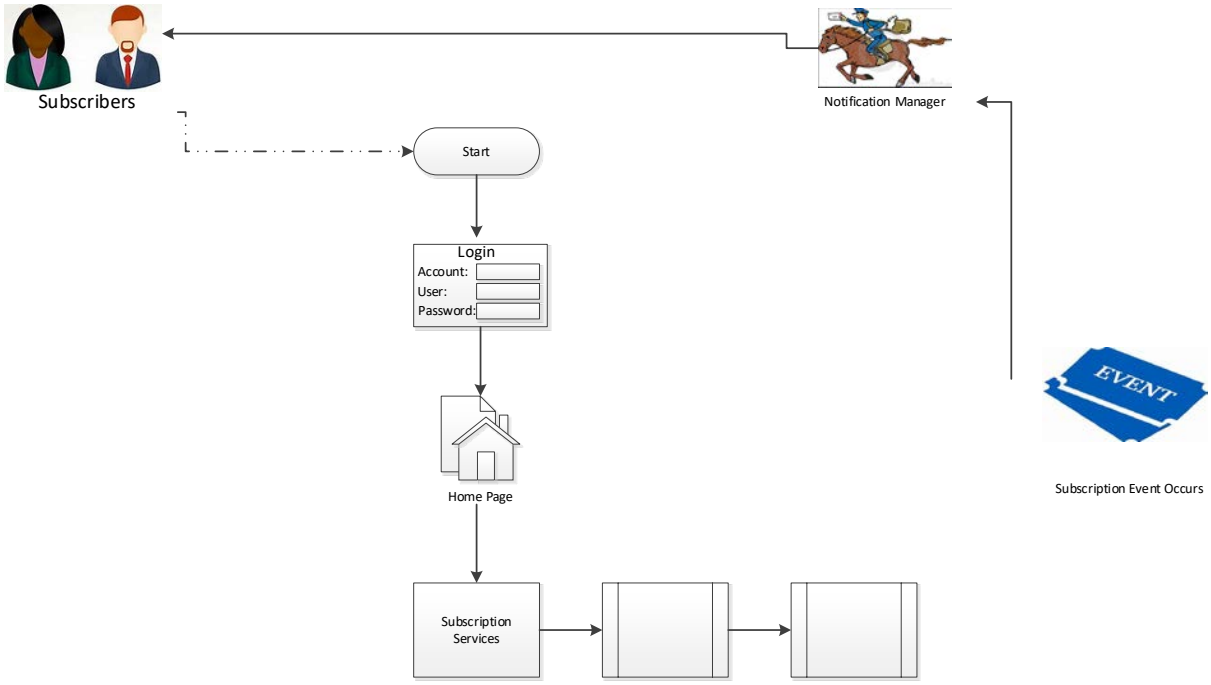
Administered Accounts



Administered Accounts



Administered Accounts



1.19.5 Functional Requirements

Ref #	Requirement	Priority
SMM 01	The administrator must be able to grant subscriptions services to an account	Mandatory
SMM 02	The administrator must be able to revoke subscription services to an account	Mandatory
SMM 03	The Account Representative can subscribe a role to request rapback services	Mandatory
SMM 04	The Account Representative can unsubscribe a role to request rapback services	Mandatory
SMM 05	The system must only allow accounts granted subscription services with the ability to subscribe roles.	Mandatory
SMM 06	The system must enforce that only roles authorized for the account can be subscribed.	Mandatory
SMM 07	The system must remove of subscriptions if subscription services for the account are revoked	Mandatory

Ref #	Requirement	Priority
SMM 08	The system must remove subscriptions if a role is no longer subscribed	Mandatory
SMM 09	The system must remove subscriptions if a role is no longer authorized for the account	Mandatory
SMM 10	CRD Staff must be able to easily lookup and locate accounts and roles that are authorized for subscription services. The lookup must offer a variety of search criteria.	Mandatory
SMM 11	The system must log all subscription management actions including the date/time, user id, account, IP address, action (request new subscription, update subscription, delete subscription)	Mandatory

1.20 Reporting Services (S)

A web portal user may be granted the rights to access reporting services, run reports and retrieve report results from their transaction history. There is no requirement for the portal to provide its own reporting services. There are two types of web portal accounts:

Public Accounts – Create and maintain their accounts. Public users do not have access to reporting services.

Administered Accounts – Users in Administered Accounts are limited in what reporting they can request and the results they can view based on the account roles assigned to the user. Authorized users can: request reports, determine the rendering and retrieve the results from their transaction history.

The work processes documented within Reporting Services include:

- Access reporting services
- Select a report and choose how it should be rendered
- Request a report
- Receive a report, Print a report. Download a Report
- Delete a report

Business Process Detail Description

1.20.1 Process Description

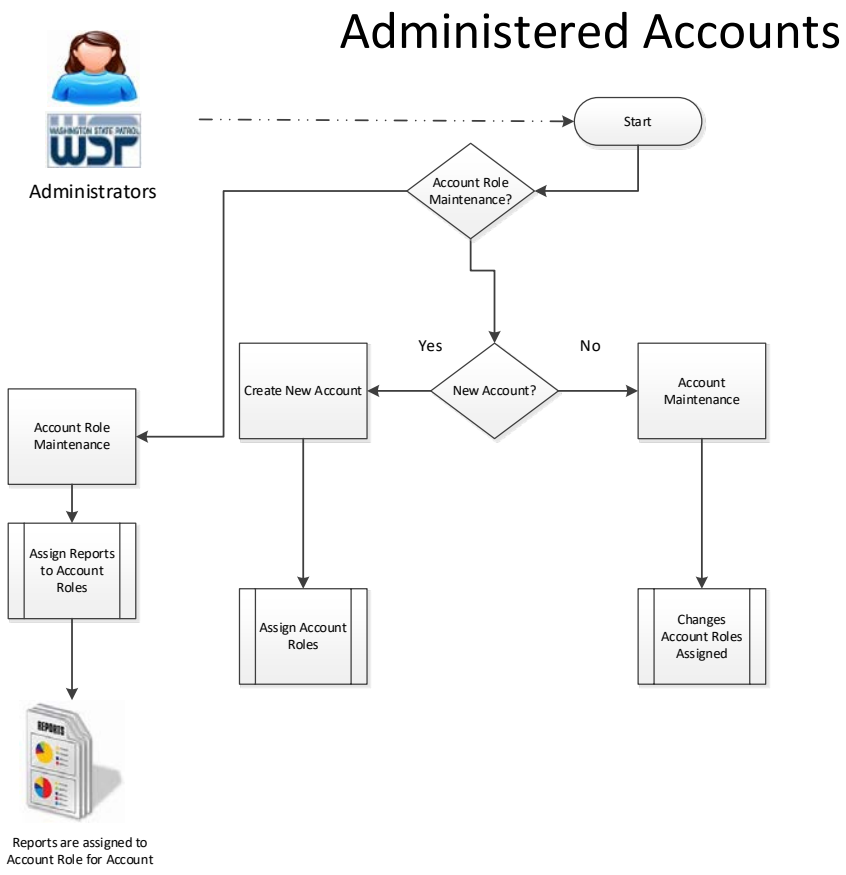
1.20.2 Actor / System

Actor	Goal
WSP Administrator	Assigns Reports to Account Roles. Assigns Account Roles to Accounts.
Account Representative	Owns and manages the transaction history. Receives notifications about transaction history.
Account User	An authorized user can pass to reporting services where they can request a report from a list of existing report, selects the criteria and chooses how the report is to be rendered. After report request is made the results are sent to the account's transaction history where they are retrieved. Account role determines the reports user can run.
System	**Purpose**
System	Enforces the access and security rules for report services. Notifies users when reporting is completed.

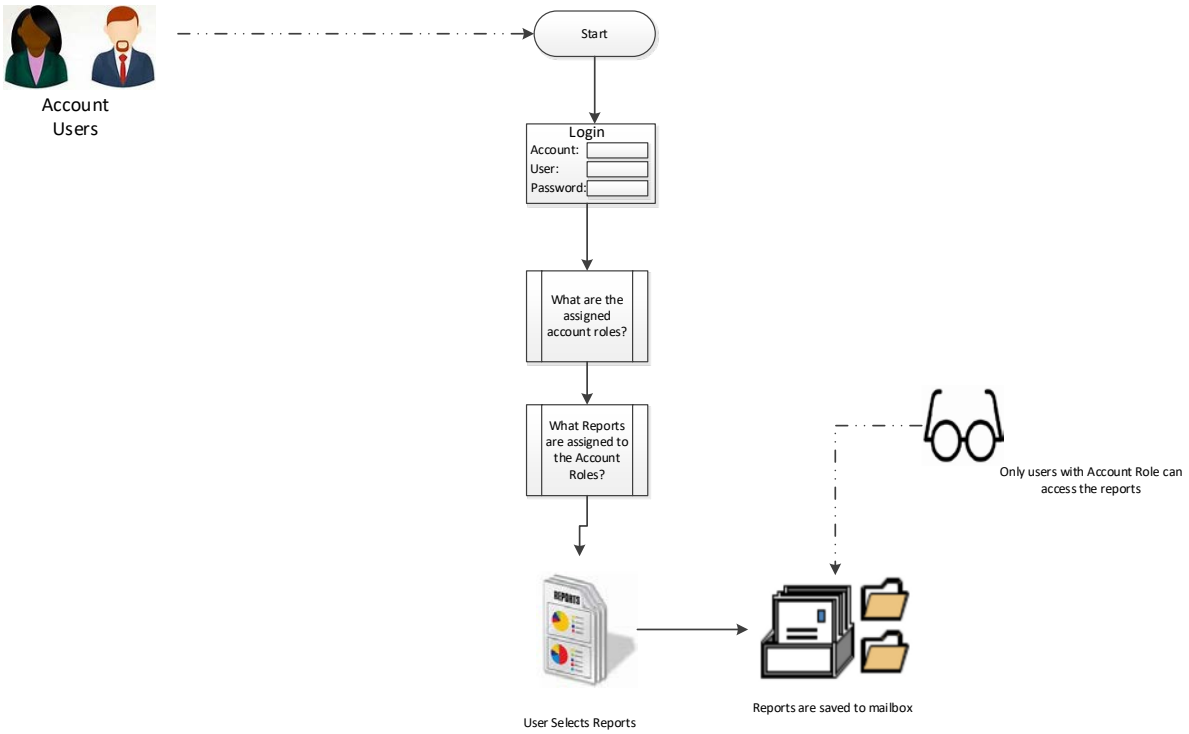
1.20.3 Triggering Events

Event Description
Account User requests a report
Account User retrieves report from transaction history and displays online
Account User prints report from transaction history
Account User downloads a report from the transaction history
Account User deletes a report from the transaction history

1.20.4 Process Steps



Administered Accounts



1.20.5 Functional Requirements

Ref #	Requirement	Priority
RSS 01	The system will control access to reports based on the account role assigned to account users	Mandatory
RSS 02	Account users select from a list of authorized reports.	Mandatory
RSS 03	Account users must be able to select the format to render the report in (html, pdf, excel, csv)	Mandatory
RSS 04	The system notifies account users when their report completes	Mandatory
RSS 05	Account users can only access reports in their transaction history that they generated or were generated by a user with the same account role	Mandatory
RSS 06	Account users can retrieve and download reports from their transaction history	Mandatory
RSS 07	Account users can delete their reports from their transaction history	Mandatory
RSS 08	CRD Staff must be able to easily lookup and audit all reporting history. The lookup must offer a variety of search criteria.	

Ref #	Requirement	Priority
RSS 09	The system must log all reporting services actions including the date/time, user id, account, IP address, action (report selected)	Mandatory

See Appendix C for samples of some of the reports available

1.21 Web Forms Management (S)

An additional purpose of the web portal is to allow customers to securely provide data to WSP through intake forms that are available on the web portal. The user enters information into the form and then submits it to the system that communicates the information to WASIS through an API. WASIS processes the information and sends a response that is captured by the system and routed to the user. There are two types of web portal accounts:

Public Accounts – Web Forms are added to the Account Roles that service public accounts. Authorized users fill in, submit the web forms. Based on the web form, they will receive a response or a notification in their message queue.

Administered Accounts – Users in Administered Accounts may fill in web forms if they are permitted by the account roles assigned to them. Authorized accounts fill in, submit the web forms. Based on the web form, they will receive a response or a notification in their message queue.

The intake form is a web form on a web page allows the web portal user to enter data that can be sent to WASIS for processing. These forms will resemble paper or database forms that are filled in by the web users using checkboxes, radio buttons, or text fields.

The work processes documented with Web Forms Integration include:

- Grant authority to Web Forms
- Fill in Web Forms
- Submit Web Forms
- Process Web Forms
- Respond to Web Form submission

Business Process Detail Description

1.21.1 Process Description

Authorized users can enter web forms that provide them with a means to fill in information, submit it to the system and receive a response that their data has been processed. WSP Administrators assign Web Forms to Account Roles.

1.21.2 Actor / System

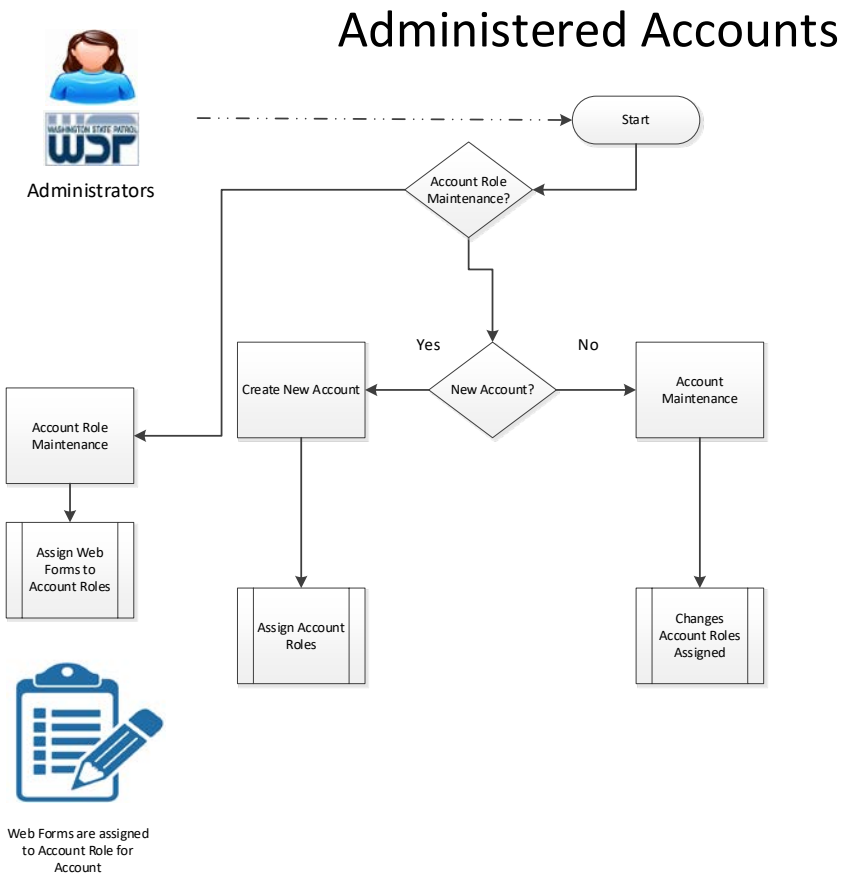
Actor	Goal
Public User	Access web form, fill in and submit to web portal and receive response from system
WSP Administrator	Has administrative control over web forms
Account Representative	Access web form, fill in and submit to web portal and receive response from system
Account User	Access web form, fill in and submit to web portal and receive response from system

System	Purpose
System	Displays web forms based on user security, processes submitted web forms and sends response back to user after submitted form processed.

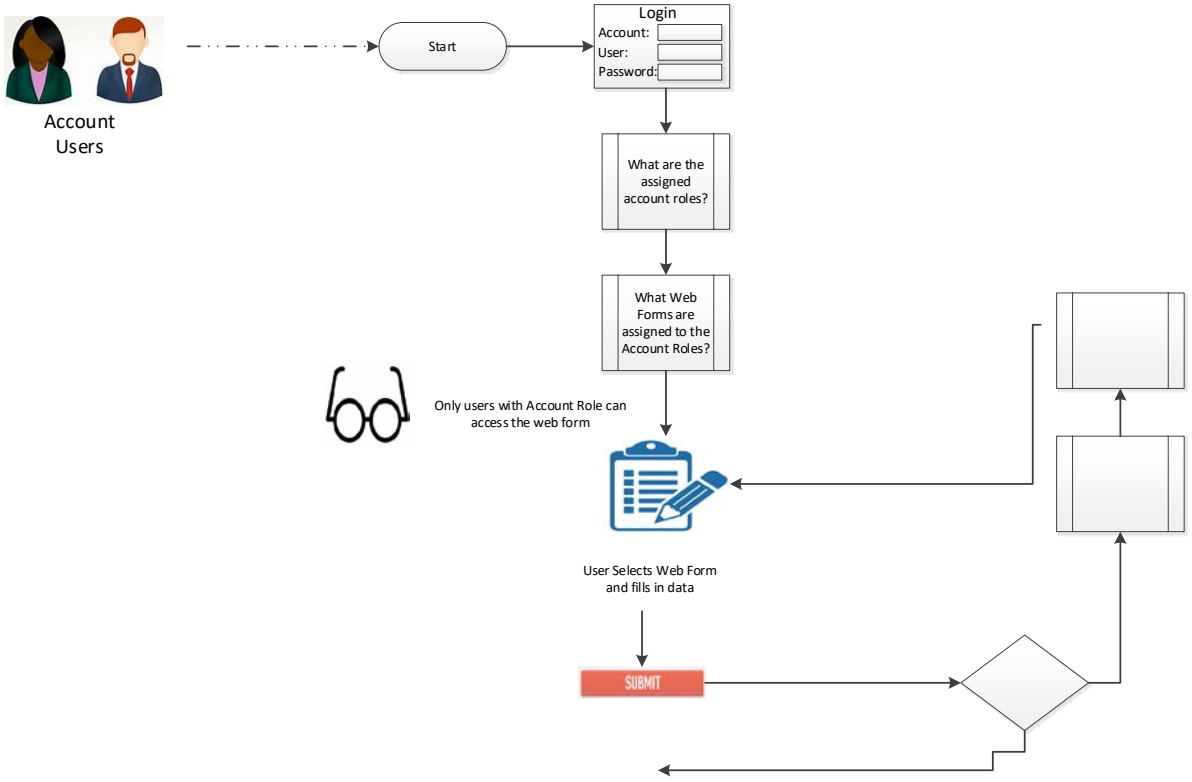
1.21.3 Triggering Events

Event Description
The Public User navigates to an authorized web form, fills in the form, submits it and may receive a response or will receive a message in their message queue.
The Account User navigates to an authorized web form, fills in the form, submits it and may receive a response or will receive a message in their message queue.
The Account Representative assigns account roles to Account Users that have been assigned web forms.
The WSP Administrator adds or removes web forms from Account Roles

1.21.4 Process Steps



Administered Accounts



1.21.5 Functional Requirements

Ref #	Requirement	Priority
WFI 01	The System must support the integration of web forms on the Web Portal	Mandatory
WFI 02	The system will limit access to web forms based on authorized account roles	Mandatory
WFI 03	The WSP Administrator will assign or remove web forms from account roles.	Mandatory
WFI 04	The system will determine the appropriate response when a web form is processed and: a.) provide an immediate response b.) provide a message in the users message queue c.) provide both an immediate response and a response in the users message queue.	Mandatory
WFI 05	The system will provide full error handling for web forms	Mandatory
WFI 06	The system will process the web form when it is submitted, test for error conditions, and once accepted initiate the underlying functions to process the data.	Mandatory

Ref #	Requirement	Priority
WFI 07	The system will log web form entries capturing the user and time stamp for each entry.	Mandatory

1.22 Document Management (S)

A web portal Account may be granted the rights to upload documents to the web portal. There are two types of web portal accounts:

Public Accounts – Create and maintain their accounts. Public users do not upload documents.

Administered Accounts – Users in Administered Accounts are limited in what files they can upload based on the account roles assigned to them. Authorized users can: upload files for specific documents and receive confirmation that the documents were successfully uploaded.

The work processes documented within Document Management include:

- Grant authority to upload documents
- Control the types and size of documents uploaded
- Upload Documents to Web portal
- Send Notification of successful uploads

Business Process Detail Description

1.22.1 Process Description

When the WSP Administrator creates an Administered Account they may grant the account authority to upload documents to the web portal. Document management is the association of a document type with an Account Role. A File Upload Interface allows the authorized users to upload load files for the associated Document Types to subfolders setup under that Administered Account on the Web Portal. Notifications of file uploads are managed through the Notification Services. The system enforces the rules for document management services. Public users do not upload documents.

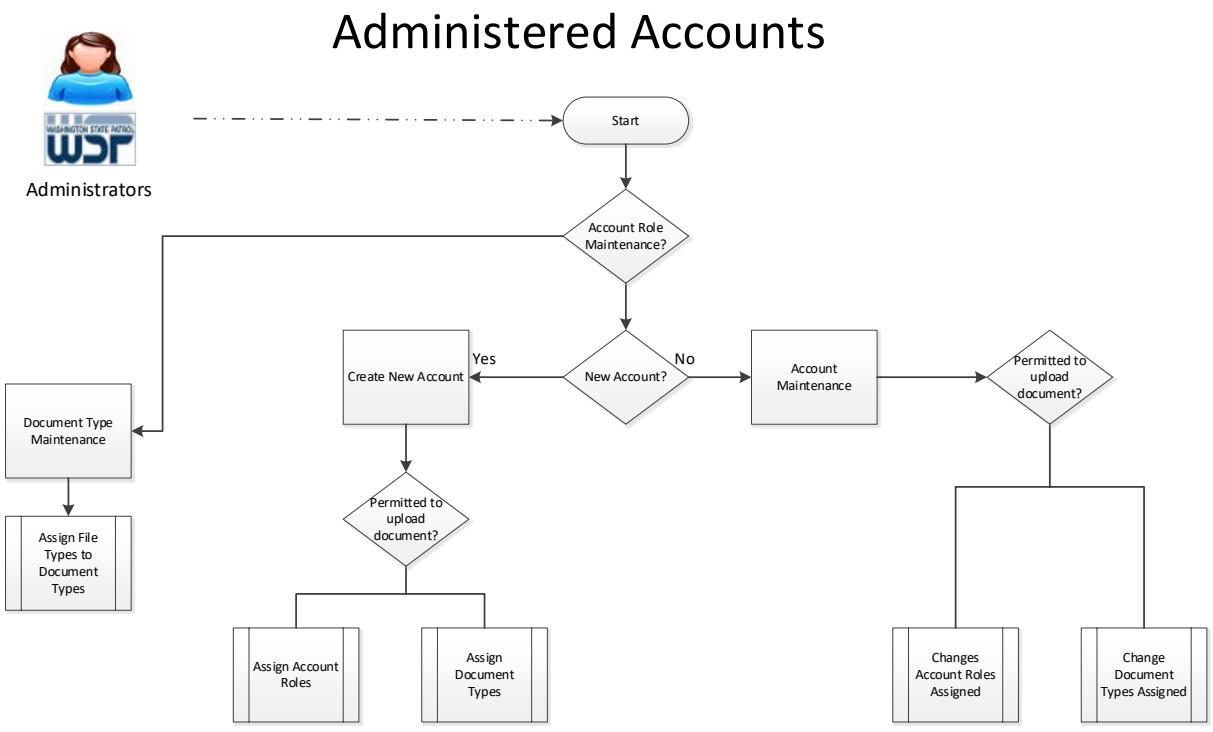
1.22.2 Actor / System

Actor	Goal
Public User	Do not upload documents
WSP Administrator	Grants, maintains, and revokes authority to upload documents for administered accounts. Assigns the valid document types for the account.
Account Representative	Assigns Document Types to Account Roles and assigns Account Roles to Account Users.
Account User	Use the File Upload Interface to upload files of the allowed document types to the Web Portal.
System	**Purpose**
System	Enforces the access and security rules for document management. Notifies users when uploads have completed.

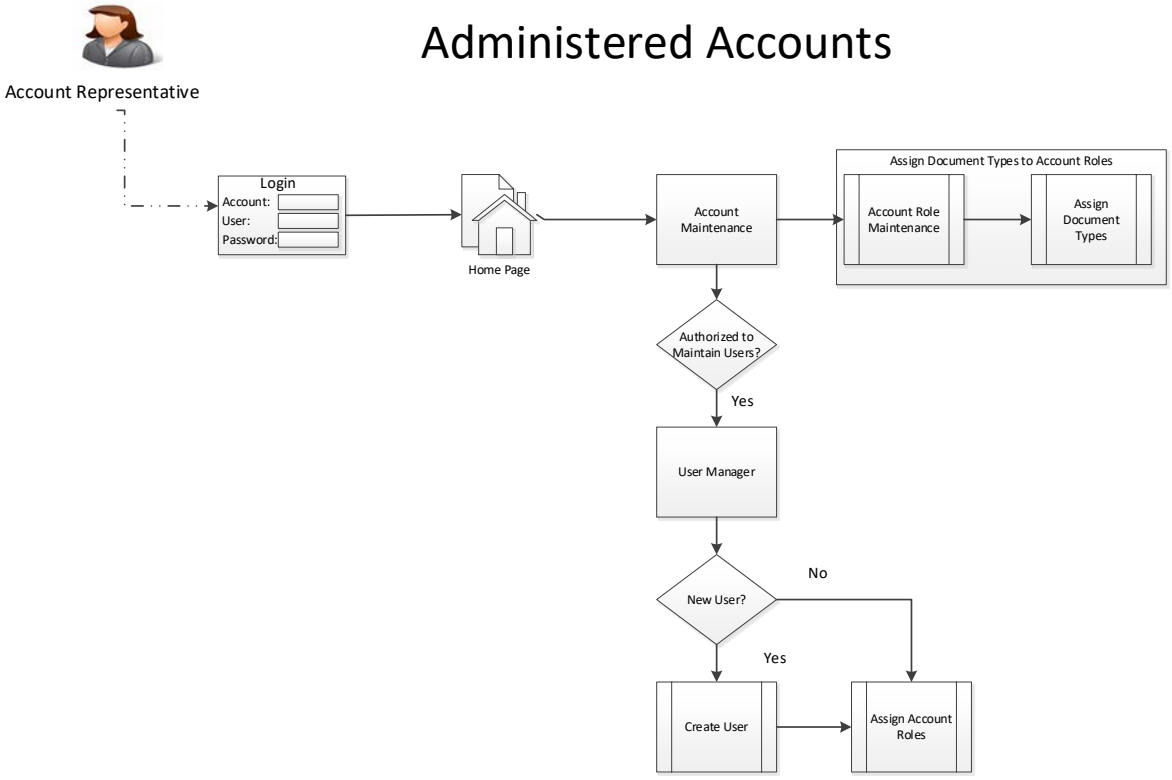
1.22.3 Triggering Events

Event Description
The WSP Administrator creates the account and grants authority to upload files
The WSP Administrator updates the account and grants authority to upload files
The WSP Administrator updates the account and revokes the authority to upload files
The WSP Administrator assigns document types to the account.
The Account Representative assigns document types to the account roles
The Account Representative assigns account roles to account users
An account user with a an account role associated with document type for an authorized account logs into the Web Portal and uses the File Upload Interface to upload files for that document type to the web portal
With the successful upload of a file, a notification is sent to the role

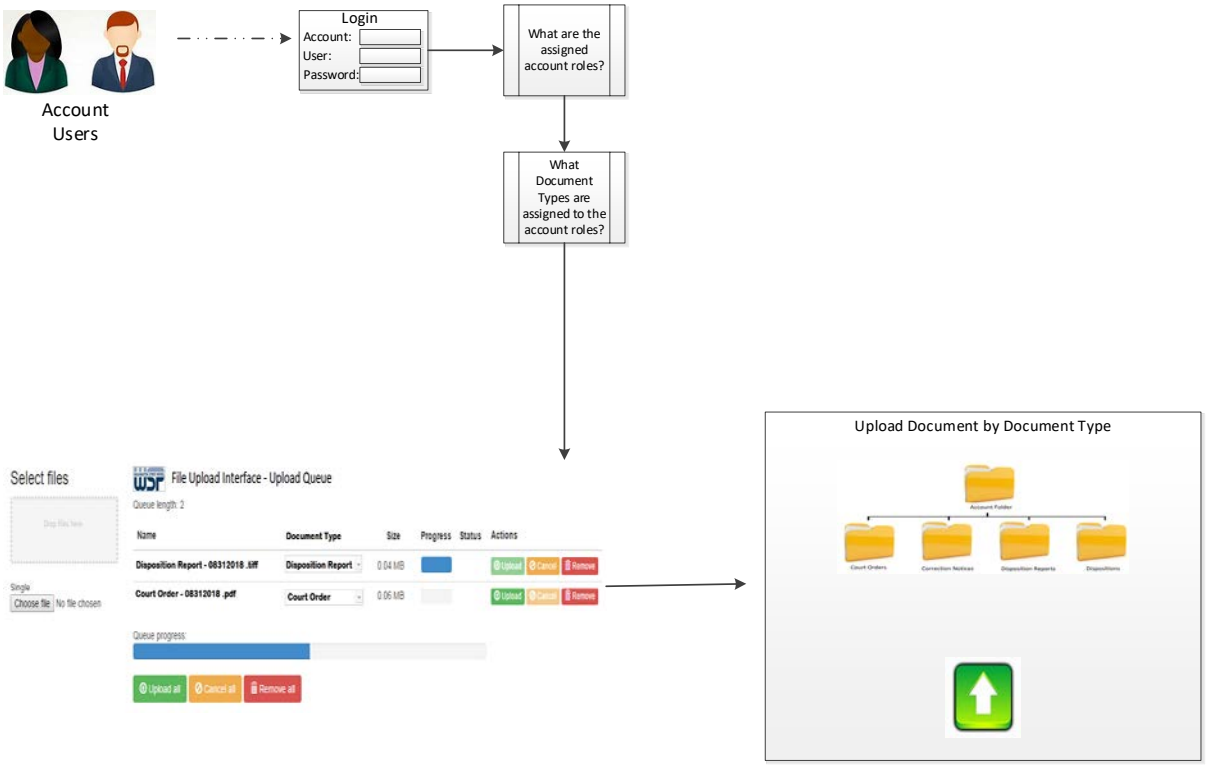
1.22.4 Process Steps



Administered Accounts



Administered Accounts



1.22.5 Functional Requirements

Ref #	Requirement	Priority
DMM 01	The system shall allow for the creation and maintenance of Document Types. Each Document Type shall include a Document Type Code, a Name, a Description, a maximum file size and a list of valid file types (pdf, tiff, csv and etc.) associated with it.	Mandatory
DMM 02	The system shall support a maintainable default file size and default file types (pdf, tiff, csv) that will be applied when document types are created.	Mandatory
DMM 03	The system shall support the WSP Administrator designating Administered Accounts as authorized to upload documents.	Mandatory
DMM 04	The system shall allow the WSP Administrator to assign Document Types for an authorized Administered Account.	Mandatory
DMM 05	The system shall allow the WSP Administrator to associate Document Types with an Account Role for an Administered Account.	Mandatory
DMM 06	The system will create a folder for each Administered Account designated as authorized to upload documents.	Mandatory
DMM 07	The system will create a subfolder for each Document Type assigned to an authorized Administered Account.	Mandatory
DMM 08	The system will grant the Account Representative permission to all subfolders created for their Administered Account.	Mandatory
DMM 09	Account Users will be granted permissions to subfolders based on the document types assigned to the account roles associated with their User ID.	Mandatory
DMM 10	The system will provide a secure File Upload Interface within the web portal that will allow authorized users to: • To select multiple files either by browsing or by dragging & dropping • To start the upload process • To cancel the upload process • To view uploaded files To delete uploaded files	Mandatory
DMM 11	The system will prompt users if the file they are uploading has the same name as an existing file in the subfolder. The prompt will allow the user to either overwrite the file or change the name of the file being uploaded.	Mandatory

Ref #	Requirement	Priority
DMM 12	The system shall prompt the user to identify the document type for the files being uploaded.	
DMM 13	The system will support file upload methodologies that can chunk the uploading of large files.	Mandatory
DMM 14	The system will support file upload methodologies that allow the upload process to resume automatically if the connection has been broken once the connection is reestablished.	Mandatory
DMM 15	The system will limit the Document Types the Account User can upload based on the Account Roles associated with the Account User.	Mandatory
DMM 16	The system will limit the size and file type the Account User can upload based on the Document Types assigned to the Account Roles associated with the Account User.	Mandatory
DMM 17	The system will determine the target subfolder to upload the files with the document type.	Mandatory
DMM 18	The system shall display the name and size of each file being uploaded and the collective size when multiple files are uploaded simultaneously.	Mandatory
DMM 19	The system shall display a message displaying the progress of the file upload such as current percentage complete. If multiple files are being uploaded it should display the status for each.	Mandatory
DMM 20	The system shall display a completion message for the successful upload of each file.	Mandatory
DMM 21	Each file in the subfolder will contain the name, file type, size, date/time uploaded and user id who uploaded the file.	Mandatory
DMM 22	The system must log all document management actions including the date/time, user id, account, IP address, action (upload file, delete file, overwrite file)	Mandatory
DMM 23	The system must revoke permissions to the file hierarchy if the account is no longer authorized to upload files.	Mandatory
DMM 24	The system must remove access to the File Upload Interface if a user no longer has any document types associated with their Account Roles.	Mandatory

Ref #	Requirement	Priority
DMM 24	CRD Staff must be able to easily lookup and locate accounts and roles that are authorized for subscription services without leaving the WASIS UI. The lookup must offer a variety of search criteria.	Mandatory

1.23 Context-Sensitive Help (CSH) Services (S)

Every web portal account must be able to launch context sensitive help (CSH) at any point in the application with a single keystroke or mouse click. CSH provides users with both application page and field-level help. Launching CSH opens a browser window that the user can size and adjust the onscreen location. After CSH is launched the user can navigate the contents using the table of contents (TOC), index or search functions. WSP Administrators can author and edit CSH content using common office tools like Microsoft Word. Updates to content are performed without requiring programming or recompiling of the web portal.

The work processes documented within Context Sensitive Help (CSH) include:

- Provide CSH at page and field level
- Navigate CSH using the Table of Contexts, Index or Search capacity
- Author and edit CSH content
- Update CSH content
- Integrate CSH with FAQs and Chatbot Services

Business Process Detail Description

1.23.1 Process Description

A web portal user (Public User, Account Representative or Account User) can launch Context Sensitive Help (CSH) to describe the purposes and actions available on a page or a specific field on a page with a specified keystroke or mouse click. Once launched the user can then navigate the contents of the CSH using the table of contents, index or search function. WSP Administrators author, edit and curate the CSH content. The system updates TOC and re-indexes the CSH when content is updated.

1.23.2 Actor / System

Actor	Goal
Public User	Launches CSH at page or field levels. Then can navigate the CSH using TOC, Index or Search
WSP Administrator	Authors and Edits CSH content
Account Representative	Launches CSH at page or field levels. Then can navigate the CSH using TOC, Index or Search
Account User	Launches CSH at page or field levels. Then can navigate the CSH using TOC, Index or Search
System	**Purpose**
System	Integrates CSH with Web Portal pages and fields. Responds to request for CSH and opens CSH function. Re-indexes and TOC after updates. Integrates CSH content with FAQs. Integrates CSH content with Chatbot.

1.23.3 Triggering Events

Event Description
The Web Portal User launches CSH through a keystroke or mouse click and the system displays the relevant help text.
The CSH user can navigate content using TOC, index or search tool to find help for a specific activity or function.
The WSP Administrator authors new content for the CSH.
The WSP Administrator edits existing content for the CSH.
The System updates changes to TOC and re-indexes the CSH.

1.23.4 Process Steps

1.23.5 Functional Requirements

Ref #	Requirement	Priority
CSH 01	The option to launch CSH will occur will begin when users reach the sign-on page for the Web Portal.	Mandatory
CSH 02	The CSH is accessible from every page in the portal.	Mandatory
CSH 03	The CSH is launched by a keystroke or a mouse click.	Mandatory
CSH 04	Launching the CSH causes the system to redirect the user to a web page with the appropriate Help content.	Mandatory
CSH 05	The user can search CSH content with a search engine.	Mandatory
CSH 06	The user can search all help content text using the search engine. The search will provide scored results for the search.	Mandatory
CSH 07	The user can navigate the CSH content using the TOC of help topics.	Mandatory
CSH 08	The user can navigate the CSH content using the Index.	Mandatory
CSH 09	The user can navigate from the CSH to FAQs, documents or tips as well as help topics.	Mandatory
CSH 10	The user can navigate the CSH without having to use the web browser navigation controls.	Mandatory
CSH 11	WSP Administrators can author or edit context using common office tools such as MSFT Word.	Mandatory
CSH 12	WSP Administrators will create and assign help topics, index words and smart links for their CSH content.	Mandatory

Ref #	Requirement	Priority
CSH 13	CSH can be activated at the page level by a keystroke or a mouse click	Mandatory
CSH 14	CSH can be activated at the field level by a keystroke or a mouse click	Mandatory
CSH 15	The system will update TOC and indexes when CSH content is updated	Mandatory
CSH 16	WSP Administrators can add link CSH content to specific fields or pages.	
CSH 17	WSP Administrators can add link documents, FAQs and smart links to CSH content.	Mandatory
CSH 18	The CSH can be configured to support pop-up windows.	Mandatory
CSH 16	The CSH must work with common browsers (Chrome, Firefox and IE).	Mandatory
CSH 17	The CSH must support changes to content without changes in the application's code.	Mandatory
CSH 18	The CSH must adhere to the inherited security model of the web portal.	Mandatory

1.24 Frequently Asked Questions (FAQ) Management (S)

A web portal user (Public User, Account Representative or Account User) must be able to navigate to Frequently Asked Questions (FAQs) at any point in the application with a single keystroke or mouse click. The FAQs framework must support the inclusion of images, email addresses and hyperlinks as well as simple navigation options to return to the original web page. The FAQ framework must support the creation of multiple FAQs to address different topics. Users can search and navigate the FAQ without using web browser navigation controls. WSP Administrators can author and edit FAQ content using common office tools like Microsoft Word. Updates to FAQ pages are performed without requiring programming or recompiling of the web portal.

The work processes documented within FAQ Management include:

- Integrate FAQs into the Web Portal
- Provide Web Users with access to FAQ pages
- Provide a home page for FAQ pages
- Provide a link to the FAQs home page on the Users home page
- Provide authoring and editing process for FAQs for WSP Administrators
- Integrate FAQs with Context Sensitive Help and Chatbot Services

Business Process Detail Description

1.24.1 Process Description

When a user enters the WSP Web Portal they need to be presented with the option to navigate to the FAQ home page. From the FAQ home page the user can navigate to individual FAQ pages for different topics. WSP Administrators author and edit FAQ pages using common office tools and the system performs updates TOC and re-indexes the CSH.

1.24.2 Actor / System

Actor	Goal
Public User	Access FAQs
WSP Administrator	Authors and Edits FAQs
Account Representative	Access FAQs
Account User	Access FAQs
System	**Purpose**
System	Integrates FAQs with Web Portal

1.24.3 Triggering Events

Event Description
The Web Portal User accesses the FAQ home page through a keystroke or mouse click and the system directs the user to the FAQ home page

Event Description
The Web Portal User once on any help text display page navigates to help home pages and uses the table of contents, index or search tool to find help for a specific activity or function.
The WSP Administrator authors new content for FAQ pages.
The WSP Administrator edits existing content for FAQ pages.
The system displays the contents of the FAQ pages.

1.24.4 Process Steps

1.24.5 Functional Requirements

Ref #	Requirement	Priority
FAQ 01	The FAQs will be accessible from every page in the portal	Mandatory
FAQ 02	The system will support multiple FAQs on specific topics.	Mandatory
FAQ 03	The user will select FAQ by topic and navigate to the page for that FAQ.	Mandatory
FAQ 04	After the user navigates to the selected FAQ they can navigate back to their prior location on the web site.	Mandatory
FAQ 05	WSP Administrators can create, update and delete FAQs.	Mandatory
FAQ 06	The system will have a process to re-index FAQs when they have been changed by WSP Administrators. This will allow FAQ information to well grouped and categorized.	Mandatory
FAQ 07	FAQ pages can include hyperlinks and embedded videos or screen shots or documents.	Mandatory
FAQ 08	The user can invoke the chat bot from any FAQ page	Mandatory
FAQ 09	WSP Administrators can create, update and delete common categories for the FAQ.	Mandatory
FAQ 10	WSP Administrators can create, update and delete groupings for FAQ information.	Mandatory
FAQ 11	FAQ must have a search function that can allow users to search by key word	Mandatory
FAQ 12	The FAQ must support individual landing pages for common questions.	Mandatory
FAQ 13	The FAQ must include a question form to the effect of: “Didn’t find your question here? What would you like to know?”	Mandatory

1.25 Error Message Management (S)

The Web portal must generate error messages that are descriptive of the error condition and are meaningful and prescriptive to the Web Portal users. Error messaging must be fully integrated with all aspects of the Web Portal. User-friendly error messages need to clearly define what the problem is, why it happened and how to solve it. WSP Administrators must be able to author or edit error messages to insure that they provide Web Portal customers with messages that address each of these subject areas. The work processes documented for Error Message Management include:

- Integration of error messaging with the Web Portal
- Authoring error messages that are targeted at Web Portal customers
- Allow for tailoring error messages at the field level
- Track changes to error messages on Web Portal.

Business Process Detail Description

1.25.1 Process Description

When a customer encounters an error message while within the WSP Web Portal they need to an optimum user experience that prevents them from being frustrated and provides them with valuable information that will prevent the error condition from being repeated. WSP Administrators tailor error messages to the user's tasks.

Actor/System

Actor	Goal
Public User	Receives error message when error occurs
WSP Administrator	Authors or edits error messages for either generic or field specific errors.
Account Representative	Receives error message when error occurs
Account User	Receives error message when error occurs
System	**Purpose**
System	Traps errors and sends appropriate error message to users.

1.25.2 Triggering Events

Event Description
The Public User performs a task in the Web Portal that causes an error condition and the system displays an error message.
The WSP Administrator writes a custom error message that will be displayed when a specific task generates an error.

Event Description
The System responds to an error condition by testing if a custom message exists for that error condition and if located displays the custom error message otherwise it will display the generic error message.

1.25.3 Process Steps

1.25.4 Functional Requirements

Ref #	Requirement	Priority
EMM 01	The system responds to an error by displaying a message on the page.	Mandatory
EMM 02	The error message displayed by the system may either be a generic error message or a custom error message.	Mandatory
EMM 03	WSP Administrators can author custom error messages for each error code trapped by the system.	Mandatory
EMM 04	The system will default to a generic error message when no custom error message is available	Mandatory
EMM 05	The system will highlight the entries (if applicable) that have caused the error condition when the error message is displayed	Mandatory
EMM 06	The system will allow users to correct their errors and reprocess the input.	Mandatory
EMM 07	The system will prevent input from processes as long as there are errors.	Mandatory
EMM 16	Custom errors messages must support for the incorporation of icons, links	Mandatory
EMM 17	The system must allow for the creation of a 404 error page message (deleted page, broken link, mistyped URL)	Mandatory

1.26 Chatbot Integration (S)

Every web portal account must be able to activate a Chatbot to provide assistance and guidance to services offered by the web portal. The web portal integrates the Chat Bot services either as a utility within the portal software or as third party software product. The requirements are applicable for either solution.

The work processes documented within Chat Bot Integration include:

- Integrate Chatbot services into the Web Portal back end systems
- Integrate Web Portal and Chat Bot Security
- Integrate Chatbot with CSH and FAQs data and services

Business Process Detail Description

1.26.1 Process Description

When a user enters the WSP Web Portal they may utilize a Chatbot that can simplify and expedite every day processes on the portal.

1.26.2 Actor / System

Actor	Goal
Public User	Can utilize Chatbot for tasks
WSP Administrator	Has administrative control of Chatbot.
Account Representative	Can utilize Chatbot for tasks
Account User	Can utilize Chatbot for tasks
System	**Purpose**
System	Integrates Chatbot with Web Portal functionality.

1.26.3 Triggering Events

Event Description
The Public User activates the Chatbot and the Chatbot guides the user through common portal activities
The Account User activates the Chatbot and the Chatbot guides the user through common portal activities
The Account Representative activates the Chatbot and the Chatbot guides the user through common portal activities

1.26.4 Process Steps

1.26.5 Functional Requirements

Ref #	Requirement	Priority
CBI 01	The option to activate the Chatbot will occur when users first successfully log onto the Web Portal.	Mandatory
CBI 02	The Chatbot should clearly identify itself as a robot and query the user what they need help with and provide a short list of potential topics.	Mandatory
CBI 03	The Chatbot should provide a date/time stamp for text responses from Chatbot and from the user in the text window.	Mandatory
CBI 04	The Chatbot should allow users to click on one of the listed topics and take the user to a list of relevant FAQ's.	Mandatory
CBI 05	The Chatbot should provide a window for user to type in what they are interested in and the Chatbot should return the following: • A sorted list of relevant FAQ's • The appropriate Help Page if appropriate	Mandatory
CBI 06	The Chatbot should present a link to an email form for technical comments, questions and inquiries regarding the WATCH website that will be sent to WATCH HELP (watch.help@wsp.wa.gov).	Mandatory
CBI 07	The email form will include First and Last Name, Daytime Phone Number, Email Address, Postal Address	Mandatory
CBI 08	Chatbot should present a link to an email form for inquiries regarding criminal history that will be sent to CRIMINAL HISTORY INFORMATION (crimhis@wsp.wa.gov)	Mandatory
CBI 09	The email form will include First and Last Name, Daytime Phone Number, Email Address, Postal Address	Mandatory
CBI 10	The Chatbot will present a "No Thanks" link which will allow the user to click on and stow the Chatbot Icon visibly to the side for all subsequent web portal pages.	Mandatory
CBI 11	When users click on the stowed Chatbot Icon, it will pop up again prominently.	Mandatory
CBI 12	After the Chatbot has provided a list of relevant links it shall query the user as to their satisfaction with the interaction and suggestions for changes to the web portal.	Mandatory

Ref #	Requirement	Priority
CBI 13	The Chatbot will access and search a text file that contains a consolidated list of web portal's FAQ's and Answers.	Mandatory
CBI 14	The Chatbot will also direct users to existing Help pages that are appropriate for the current page that the User is accessing.	Mandatory
CBI 15	The Chatbot Administrative Interface shall provide a WSP Administrators administrative control of the Chatbot Solution. The interface will utilize the Web Portal security to identify the WSP Administrators who are authorized to access the Administrative Interface.	Mandatory
CBI 16	The Chatbot Administrative Interface shall authorize WSP Administrators to update the web portal FAQ's and Answers in real time and without involvement of Technical Staff.	Mandatory
CBI 17	The Chatbot Administrative Interface shall provide on demand reports listing the content of and numbers of user questions, inquiries and satisfaction surveys.	Mandatory
CBI 18	The Chatbot Administrative Interface shall provide on demand reports listing survey results and suggestions for improvements.	Mandatory
CBI 19	The Chatbot shall have the capability to launch and manage chat sessions with WSP authorized staff.	Mandatory
CBI 20	The Chatbot shall have the capability to support outbound audio through the browser session.	Mandatory
CBI 21	The Chatbot shall have the capability to provide support for avatars	Mandatory
CBI 22	The Chatbot shall have the capability to provide support for texting interactions with Users.	Mandatory

2 APPENDIXES

2.1 Appendix A – Account Roles

Account Roles group tasks performed by customers and provide a table driven means of granting privileges for a common sets of those tasks. An individual user may be assigned more than one account role. WSP Administrators determine what account roles are appropriate for an Administered Account and once they have assigned those roles to the account, an Account Representative can assign account roles to individual users from the list of valid account roles.

The users of Public Accounts are all assigned the account role of Public Account by the system when they establish their account. This role grants them administrative rights to their account and transaction history.

When the WSP Administrator establishes an Administered Account they select what account roles are valid for the account. They assign the account role of Agency Contact to the Account Owner and the role of Account Representative to the Account Representative. The Account Representative role grants the Account Representative the authority to assign designated account roles to the users. The special account role of Account Representative (Restricted) is for those Account Representatives that are not granted rights to create or modify users or assign account roles to them. The remaining account roles are groups around specific tasks they perform for their agency.

The following are examples of some identified account roles expected to be used for the WSP Web Portal.

Account Role	Assigned by
Public Account	System
Agency Contact	WSP Administrator
Account Representative	WSP Administrator
Account Representative (Restricted)	WSP Administrator
ABIS Coordinator	Account Representative
ACCESS Coordinator	Account Representative
SOR Coordinator	Account Representative
Billing Management	Account Representative
HR Coordinator	Account Representative
Auditing Coordinator	Account Representative
Rapback Coordinator	Account Representative
Rapback Subscriber	Account Representative

2.2 Appendix B - Interface Types

Interface Types Abbreviation	Description

WEB	Public Account
CJA	Criminal Justice Agency
WS	Washington State Agency
HUD	Federal Department of Housing and Urban Development

2.3 Appendix C - Payment Methods

Account Role	Description
Pre-Paid	Services are charged to credit card
Billed	Invoiced for services
Non-Billed	Not invoiced for services

2.4 Appendix D - Types of Background Check Results

Types of Background Search Results	Description
Exact Match Available	An Exact MATCH was found for the exact name and date of birth the search criteria used.
Candidate List	A list of records that match or closely match the search criteria.
No Record Found	There is no conviction record in the WSP database that match the search criteria used. The system found no candidate based on the search criteria.
No Exact Match Found	There is no conviction record in the WSP database that exactly match the search criteria used. The system did return a candidate based on the search criteria that is a possible match.
Duplicate Match	A possible DUPLICATE MATCH indicating that there may be two or more exact name and/or date of birth matches for the search criteria used.
Conviction Only	A transcription comprised of records sent to WASIS by courts and criminal justice agencies throughout the state of Washington only. This includes conviction information, arrests less than one year old with dispositions pending, and information regarding registered sex and kidnap offenders.
Non-Conviction	Non-conviction information is not available to the public. It is information is CHRI which has not led to a conviction or other disposition adverse (negative) to the subject. A transcription comprised of records sent to WASIS by courts and criminal justice agencies throughout the state of Washington only. This includes conviction and non-conviction information, arrests less than one year old with

	dispositions pending, and information regarding registered sex and kidnap offenders.
Search Failed	The search failed for technical reasons, no valid results were returned and the account should not be charged for the search.

2.5 Appendix E – Examples of Reports

The following are samples of some the types of reports that should be available to authorized users of the Web Portal.

	Reports	Access
	Transaction History	Administrator
	Transaction Totals	Administrator
	Aggregate Searches by Account User	Administrator
	Users by Account Role	Administrator
	SOR Reporting	SOR Coordinators

2.6 Appendix F – Fingerprint Reason Code

These are examples of the codes categorize the reason for the fingerprint background check.

	Fingerprint Reason Code
	ALIEN FIREARM LICENSE WARC 9.41.170
	APPLICANT STATE INVESTMENT BOARD
	CARD ONLY
	CHILD ADULT ABUSE (PROFIT)
	CHILD ADULT ABUSE (NON-PROFIT)
	CONCEALED PISTOL LICENSE
	CRIMINAL JUSTICE APPLICANT
	CRIMINAL JUSTICE INVESTIGATIVE PURPOSE
	DEPARTMENT OF CORRECTIONS
	ENTERTAINERS LICENSE
	INQUIRY DOCUMENT - NON CONVICTION
	LOCAL ORDINANCE
	PUBLIC INFORMATION
	PUBLIC INFORMATION - NON CONVICTION
	TAXI LICENSE
	6401 MEDICAID

2.7 Appendix H - Applicant Type

These are examples of the categories of the applicant process.

	Description
	Background
	Criminal Justice
	Department of Information Services
	Department of Transportation Employee
	Fingerprint Services Printing

	United States Department of Housing and Urban Development
	NDOB Background Check
	On-Site Vendor
	Notary
	No Application Type
	Personal Identification
	Record Review
	Research Agreement
	Search and Return
	State Applicant - No Charge
	State Applicant - User Fee
	State & FBI Applicant - User Fee

2.8 Appendix I – Types of Transactions

Code	Transaction Description
FANC	Federal Applicant, No Charge
FAUF	Federal Applicant, User Fee
FPSV	Fingerprint Service
LVSC	Livescan Submission
MAP	Miscellaneous Applicant
NDOB	Name, Date of Birth
NFUF	Non Federal User Fee
NTRY	Notary Processing
WHV	WATCH High Volume
WTC	WATCH

2.9 Appendix J – Definition of Terms and Acronyms

This section provides definitions of terms and acronyms.

Term or Acronym	Definition
ABIS	Automated Biometric Identification System. Previously referred to as Automated Fingerprint Identification System (AFIS).

ACCESS	A Central Computerized Enforcement Service System (State Message Switch).
Background Check	The process of checking if a person has a criminal record
BFS	WSP Budget and Fiscal Services. BFS manages WSP contracts and procurements.
BGU	Background Check Unit. The BGU is a unit within the WSP's Criminal Records Division.
CCH	Computerized Criminal History System
CHDAR	Criminal History Document Archive and Retrieval.(see ILINX)
CHRI	Criminal History Record Information
CHSU	Criminal History Support Unit. The CHSU is a unit within the WSP's Criminal Records Division.
CIC	Crime Information Center
CJIS	Criminal Justice Information Services. CJIS is a division of the FBI that operates national NCIC and III services.
Criminal Justice	Criminal Justice is composed of 3 segments: (1) law enforcement; (2) adjudication; and (3) corrections; that operate together under the rule of law.
CPL	Concealed Pistol License
CRD	Criminal Records Division of the WSP
CSH	Context Sensitive Help
DOB	Date of Birth
DOC	Department of Corrections
DOT	Department of Transportation
FAQ	Frequently Asked Questions
FBI	Federal Bureau of Investigation
FBI#	A Unique Number assigned by the FBI to a person with a criminal record
HR	Human Resources
HUD	United States Department of Housing and Urban Development
ILINX	WSP Document Imaging System used by CRD to store images of criminal justice documents, particularly judgment and sentencing documents from the courts.

IO	Infrastructure Operations Section. IO is a unit within the WSP's Information Technology Division. This unit manages the ITD servers and data center.
ITD	Washington State Patrol Information Technology Division
LEA	Law Enforcement Agency
NCIC	National Crime Information Center
NDOB	Name and Date of Birth
NIEM	National Information Exchange Model
Nlets	International Justice and Public Safety Network. Nlets is the nationwide interstate justice and public safety network that is used for the exchange of law enforcement-, criminal justice-, and public safety-related information.
OCIO	Office of the Chief Information Officer. This is the Washington State office responsible for state technology policy. See https://ocio.wa.gov/
RAP	Record of Arrests and Prosecutions
RAPback	A federal program that can inform an employer or other designated entity when an individual who has undergone a fingerprint-based background check, and whose fingerprints are retained by a criminal history repository after the check, is subsequently arrested.
RCW	Revised Code of Washington. The RCW is the compilation of all permanent laws now in force in Washington State.
RFP	Request for Proposal
RFP Coordinator	The sole point of contact in WSP for the W2 Replacement Procurement
SID	State Identification Number. This is a unique number assigned to a subject once the first set of retainable fingerprints has been received.
SME	Subject Matter Expert
SOR	Sex Offender Registry
SOR Coordinator	A state required position at each Sheriff's office in Washington State that works with SOR Unit at CRD.
SOW	Statement of Work

SQL	Structured Query Language. A programming language used to access data in a relational database.
State	State of Washington
TOC	Table of Contents
TOT	Type of Transaction
W3	This term represents WASIS, WACIC and WATCH applications and the hardware, network and other services that support the three applications.
W2 Replacement Project	A project by WSP to replace both its current CCH (WASIS) and CIC (WACIC) applications.
WATCH	Washington Access to Criminal History is a public facing interface that allows parties to conduct Name / Date of Birth background checks against the WASIS database. It has four components: WATCH Public Access WATCH CJ Criminal Justice WATCH WS WA Agencies WATCH HUD Federal: HUD
WASIS	Washington State Identification System. Contains identification and information about arrests and criminal disposition and adjudications of court actions. Arrests and dispositions are based on SID number, which is fingerprint based.
WACIC	Washington State Crime Information Center. Data source for the ACCESS network. All transactions to WACIC arrive via the state message switch. Current CIC for Washington State, also known as "hot files". Files contain information on: wanted persons, person of interest, protection orders, monitored population registration, pawned articles and guns, vehicles, license plates and impounded vehicles.
WEBS	Washington Electronic Business Solution https://fortress.wa.gov/ga/webs/
WSP	Washington State Patrol
UI	User Interface