

ROSS DISPATCH

BASIC 1 – ROSS SECURITY PRINCIPLES

OBJECTIVES

Upon completion of this unit, the trainee will be able to:

1. Identify key ROSS security principles.

I. ROSS SECURITY BASICS

- ROSS is accessible to anyone with Internet access and a ROSS User Account. ROSS Web Status accessible to anyone with Internet access and a ROSS Web Status Account.

- If have both a ROSS User and ROSS Web Status account, they use same username and password. Security rules for ROSS User Accounts also apply to Web Status Accounts.

- Each ROSS User Account consists of a unique username and a password (password does not have to be unique).

- You must always work in ROSS under your own username and password.

- Never allow another person to use your session of ROSS.
 - Documentation in ROSS stamped with date and user's name.
 - You will be responsible for any actions taken by other users while logged into your account.
 - Expectation is that you are able to explain all actions taken in your user account.

- If you leave your workstation unattended, you must either:
 - Lock your computer by use of a password.
 - Log off of ROSS.

- Before logging onto *Production*, each user must have completed Security Awareness Training (SAT).

- If suspect security breach of ROSS system, immediately report it to ROSS System Administrator or a member of IRM staff in their office.

- Beginning with ROSS version 2.14.1, ROSS will utilize services of shared NESS LDAP for user authentication (i.e., verifying identity of individual) and user account authorization (i.e., applications the account has access to, and whether access is Standard or Privileged). This change applies to suite of ROSS applications (i.e., ROSS, Web Status, Cognos Reporting, Resource Clearinghouse, and Enterprise Service Bus (ESB)).

- Following must now be performed via NESS Application Portal (NAP):
 - User creation and maintenance.

 - User account creation and maintenance.

 - Username retrieval.

 - Password change and reset.

- Whenever receive a Change Password or Login Failed message, a link to NAP is provided and following displayed: “WARNING: ROSS will shut down once the NESS Security Portal link is clicked.” Clicking link launches NAP in a web browser.

- NAP is discussed in detail in *CW – NAP – Reference Manual.docx*; only key information is repeated here.

- After logging into NAP, receive message if your acceptance of the user account’s Rules of Behavior has expired or is set to expire in 10 days or less, and link is provided to NAP.
 - ROB identifies users’ information security responsibilities.

 - Must accept at least annually.

- Automatic Log Off:
 - Session Time Out – If you do not use your mouse or keyboard for 3 hours, your ROSS session is ‘timed out’ and terminated, you are automatically logged off, and you must log back in. Any unsaved work is lost.

 - ROSS Recycle – Current users receive a warning message 5 minutes before the ROSS system is to be recycled. Save your work and log off. Any remaining users are automatically logged off prior to the recycle, and unsaved work is lost.

- The Password Reset Service (PRS) is now obsolete and has been removed.

II. USER ACCOUNT TYPES AND STATUSES

- Two types of NAP user accounts: Standard and Privileged.

- A user must have at least one user account (of either type).

- A user can have only one Standard user account with a status of Active, Temporary Password, Expired Password, Locked, or Disabled (i.e., a status other than Removed) at a time, and only one Privileged user account with a status other than Removed at a time.

- **Standard** User Accounts:
 - Provide access to perform regular dispatch job duties in ROSS.

 - Can have any user account sub-types assigned (e.g., ROSS User, OH Web Access, and Services Access).

 - Can only have Standard roles assigned:
 - In ROSS, any Security Role not designated as Privileged on Reference Data screen is a Standard role.
 - In the RC, the Standard roles are Data Steward Access and Read Only Data.

- **Privileged User Accounts:**
 - Provide access to perform administrative tasks in ROSS.

 - Can only have user account sub-type of ROSS User assigned.

 - Can only have Privileged roles assigned:
 - In ROSS, Security Roles are designated as Privileged on the Reference Data screen.
 - In the RC, the Privileged role is Administrator.

- User account statuses for which user can authenticate via NESS LDAP:
 - Active.

 - Temporary Password.

- User account statuses for which user cannot authenticate via NESS LDAP:
 - Locked (due to too many failed logins).

 - Expired Password (due to password not being changed within: 60 days for a Standard user account, or 30 days for a Privileged user account; password must be reset).

- Disabled (due to no login for 90 days or manual disabling because temporarily not needed).
- Removed (manually removed because no longer needed; precursor to account deletion).

III. USERNAMES

- Usernames are automatically generated by the system based on the user's First, Middle, and Last Names.
- If a user has both a Standard and Privileged user account, each account must have a unique username.

IV. PASSWORDS

Temporary Passwords – Randomly generated by system when any of following occur. Must be changed by user upon login.

- A user account is created or reactivated.
- A password is reset.
- Changes to a user's First, Middle, and/or Last Name result in generation of a new user account.

Password Contents – Passwords must contain:

- 12 – 32 characters.
- At least one upper-case alphabetical character.
- At least one lower-case alphabetical character.
- At least one numeric character.
- At least one non-alphabetical/non-numeric character:

~	(Tilde)	{ }	(Braces)
`	(Back Quote)	[]	(Brackets)
!	(Exclamation)		(Pipe)
@	(At)	\	(Back Slash)
#	(Number)	:	(Colon)
\$	(Dollar)	;	(Semi-Colon)
%	(Percentage)	“	(Quote)
^	(Carat)	‘	(Apostrophe)
&	(Ampersand)	< >	(Greater/Less Than)
*	(Asterisk)	,	(Comma)
()	(Parenthesis)	.	(Period)
_	(Underscore)	?	(Question)
-	(Dash)	/	(Forward Slash)
+	(Plus)		(Space)
=	(Equal)		

Logging In

- If user enters incorrect password five times in a row, account is temporarily ‘locked’ (but account status remains unchanged), and either 15 minutes must pass for account to automatically unlock, or account can be unlocked by resetting password. If user again enters incorrect password five times in a row, account status changes to Locked and password must be reset (no automatic unlock).
- No ‘grace’ logins (i.e., logging in with an expired password) are allowed.

Password Expiration

- Standard user account passwords expire every 60 days (must be changed at least every 60 days).
- Privileged user account passwords expire every 30 days (must be changed at least every 60 days).
- You begin receiving a “password will expire” message 10 days before your password is set to expire.

Password Changing

- Users can change own password as long as user account is allowed to authenticate via NESS LDAP (i.e., status of Active or Temporary Password).
- Users change password via either:
 - Password Management panel of Edit My User Account pop-up (click User icon on NAP screen).
 - Change Password pop-up, which opens automatically when a user logs into NAP with a temporary password.
- If you need help changing your password, contact ROSS Help Desk.
- Users must wait 24 hours in between password changes.

- New password:
 - Cannot match any of 24 previous passwords on the account.
 - Must contain at least one different character from previous password.
 - Must be kept secure (e.g., not on sticky notes on computer).
 - Is case sensitive, so enter it each time exactly same way it was created.

- When password of a ROSS user is changed or reset, NAP notifies ROSS of the change. Additionally, if user account is Standard and has sub-type Services Access assigned, NAP notifies affected external systems.

Password Resetting

- Users can reset own password via Reset Your User Password Pop-Up, accessed by 'Forgot Password?' link on Login screen, after first setting up a Security Profile (via Edit My User Account pop-up).

- Password Reset Managers can reset password of another user via Reset Password right-click menu item on Account Management – Manage All Accounts screen.

V. MANAGING USERS AND USER ACCOUNTS

To add a user account to a ROSS dispatch:

- If individual is not yet a user in NAP:
 - Individual requests a user account by clicking Request User Account link on NAP Login screen.

- A NAP Account Manager approves request in NAP after validating user's identity and need for the user account.

- NAP Account Manager creates the user account in NAP and authorizes access to ROSS application.

- NAP emails user account username to the individual and appropriate ROSS Account Manager.

- Once individual is a user in NAP:
 - Appropriate ROSS Account Manager searches for NAP user on User Accounts screen, selects appropriate user account (if user has both Standard and Privileged accounts, each displays separately), and adds user account to the ROSS dispatch. User accounts with a status of Removed or Disabled do not display.

 - If the individual is not already a user at another dispatch, ROSS assigns current dispatch as individual's Managing Dispatch (i.e., first dispatch to add the user to ROSS becomes user's Managing Dispatch).

 - ROSS Account Manager designates applicable user account sub-types (e.g., ROSS User, OH Supervisor), and assigns roles as appropriate.

 - When a Privileged user account is added to a dispatch, the ROSS User sub-type is automatically checked and cannot be unchecked, and no other sub-types can be assigned to the user account.

To add a user to the RC:

- Individual must be a NAP user with a user account that is authorized to access the RC. User account status cannot be Removed or Disabled.
- RC Administrator searches for NAP user on User screen and adds them as an RC user.
- RC Administrator assigns roles as appropriate.

To remove a user account's access to ROSS:

- Either the ROSS user or appropriate ROSS Account Manager notifies a NAP Account Manager that user account no longer requires access to ROSS.
- NAP Account Manager edits the user account in NAP to remove access to ROSS.
- NAP notifies the ROSS user and appropriate ROSS Account Manager when access has been removed.
- ROSS Account Manager logs into user's Managing Dispatch in ROSS and unchecks 'ROSS User' sub-type check box for the user account on User Accounts screen.

To remove a user account from a ROSS dispatch:

- Appropriate ROSS Account Manager logs into the dispatch and removes user account from User Accounts screen.

To remove a user and all associated accounts from ROSS:

- Appropriate ROSS Account Manager logs into user's Managing Dispatch and removes all of the user's accounts from User Accounts screen. This automatically removes the user from ROSS and removes the user's accounts from all other dispatches.

To remove a user from the RC:

- RC Administrator searches for the user on User screen and removes them as an RC user.

Updating user and user account information:

- Changes made to a user's first, middle, and/or last name in NAP are automatically applied to the user's information in ROSS.
- Changes made to a user account username in NAP are automatically applied to the user account in ROSS.
- Notification is sent by ROSS to affected external systems when any of following occur:
 - A ROSS role having Invoke Services function is added or removed to/from a user account in ROSS.
 - User account sub-type of either ROSS User or Services Access is removed from a user account in ROSS.
 - A user account is removed from ROSS.

- Username is changed, or password is changed or reset, in NAP for a ROSS user account.