# New SHIP NPR Account Security Management

## New Password Procedures

Changes have been made to the SHIP NPR website to implement new security measures required by CMS. The changes include new password requirements as well as new account management procedures. Additionally, users will now be able to change their email addresses and passwords directly on the SHIP NPR website. The following changes will take effect on September 04, 2012. The changes are detailed below. Please note that **bolded text** indicates an item of particular importance.

## Password Composition

The current SHIP NPR password requirements are not entirely compliant with CMS' security requirements. SHIP NPR users will be required to create more secure passwords. The goal is for users' passwords to not be so simple that they can be guessed or quickly "cracked." **Once the new security measures are implemented, dictionary words, email addresses, and names will no longer be permitted for passwords.**

### A. Minimum Security Requirements

According to the new SHIP NPR password policy, all passwords must meet the following minimum security requirements.

1. **A** password must:
    a. Be at least **eight (8)** characters
    b. Contain at least one **UPPER case** letter
    c. Contain at least one **numeric (a number)**, and
    d. Contain at least one **special character** (e.g., "! # $ % & ' ( ) * + , / : ; < = > ? @ [ \ ] ^ ` { | } ~ ] ) . * $)
2. A password **cannot use** dictionary words or names (e.g., people, pets, schools, etc.).
3. A password must have **at least four (4) characters** that are different from the previous password.
4. A password can be up to 30 characters long.
5. A password cannot be the same as any of the previous six (6) passwords. For details, see the reuse restrictions within the section "*Password Lifetime, Expiration and Reuse*".

### B. Creating A Strong Password

There are several ways to create a strong password. This section describes methods to consider using when creating a new password.

- **Substitution:** Use a word but substitute letters with characters. For example, the word "Security" is not accepted as a password because it is a dictionary word and does not contain any numbers or special characters. However, **5ekL1ri+y** looks like the word "security" and is acceptable because it substitutes **5** for S, **k** for c, **L1** for U, and a + for t. Many security resources recommend this method, which is called "Leet" or "Leetspeak." One resource for more information on this is the Wikipedia entry on Leet (http://en.wikipedia.org/wiki/Leet).

- **Passphrase:** Use a phrase, instead of a single word. For example, the phrase "Forget your Password" is not accepted as a password because it contains dictionary words and does not contain numbers or special characters. However, you may use this phrase as a foundation, and add some substitution (as described in the previous example) to create a passphrase. In this instance, the phrase could become **F0rge7 Ur Pas5woRd!** The length is of this new password is 19 characters and it contains upper case letters, numbers, and special characters.

- **Random Words:** Create a password by using a few random words together. These can be the first words that pop into your head or the first words from several articles or headlines from news sites that change frequently. For example, you could start with Heiress and Congressman, which are words from a news site, and refine them using substitution (as described in the previous example) to become **#e1re5s!** and **(0ngreSsm@n**. In this instance, the new passwords contain letters, numbers, and special characters but avoid dictionary words and minimizes use of same characters.

## C. Additional Guidance On Passwords

Here is some additional guidance and information that all users should know.

- **Do not use your SHIP NPR password with any other websites.**
  - You may have heard of recent password break-ins on other websites, so we strongly recommend that you do not use the same password on SHIP NPR that you use for other websites (e.g., email, online banking).
  - Statistics from a study for credit fraud and identity theft show that:
    - A quarter of people use the same password for most of their profiles.
    - Four percent of people use the same password for ALL of their profiles.
    - To fix this, use one password for work, a different password for personal online banking, a third password for personal email, and so on as needed.
- Other possible password creation methods and examples can readily be found with internet searches. Some guides and resources on good and bad passwords include:
  - https://www.grc.com/passwords.htm,
  - http://www.microsoft.com/security/online-privacy/passwords-create.aspx
  - http://en.wikipedia.org/wiki/Password_strength
  - http://www.youtube.com/watch?v=VYzguTdOmmU

- **Password Generators:** There are many available "Password Generators" (websites that generate and suggest passwords) but **these should be used with caution or even skepticism**. These password generators could be inadvertently providing multiple people the same password, or could be inadvertently or maliciously recording the provided password.

### D. Password Practices To Avoid

The following passwords are examples of bad passwords:

- Abcd-1234 (an alphabet sequence)
- Asdf-890_ (a sequence on keyboard)
- SHIPsunk! (a dictionary word, employer name)
- Passwords with 0 and 1, which are the most common first characters in passwords

The following should **never** be the password or part of the password, regardless of capitalization:

- 123456, 12345678, or 123456789 (etc.)
- Password
- Welcome
- Ninja
- Sunshine
- Princess
- Qwerty
- Monkey
- Jesus
- Love, freedom
- Money
- Any calendar word (for examples, April, March, Tuesday, Week, "holiday", Christmas, 2012, 1999, 1987, 1975, etc.)
- Names (boys, girls, pets, sports teams) and their nicknames (nat, nats, pat, pats, jags, etc.)
- The system or Organization/employer

## Password Lifetime, Expiration and Reuse

- **Maximum Lifetime and Expiration:** The longer a password remains unchanged, the greater the possibility of improper disclosure through accidental or malicious intent. **SHIP NPR will allow a <u>Maximum Lifetime</u> of sixty (60) days, at which time the password will expire**. **You will be required to change your password every 60 days.** Five days before your password expires, you will see a message on the SHIP NPR website informing you to change your password. If you do not change your password before it expires, your account will be locked and you will have to change your password before you log in to the website next, similar to the way you reset your password if you have ever forgotten it. Instructions for changing a password are included below, under the section titled "*Account Management and Automation*."

  Users will not be able to change their password more than one time per day. If you try to do so, you will receive the following message:

  You are not allowed to change your password more than once in a day.

This simply means that a new password cannot be changed until at least 24 hours later. This restriction applies to changing a password as well as using the Forgot Password link. This means that a user cannot perform a combination of multiple password changes and use of the Forgot Password link. If a user locks his/her SHIP NPR account, the user must wait for an hour to be able to unlock the account.

- **Reuse Restrictions:** Lastly, the SHIP NPR website has implemented Reuse Restrictions. Users cannot reuse any of their six (6) previous passwords. A password can only be reused when it is no longer one of the previous six passwords.

## Account Inactivity and Suspension

Accounts that are inactive for long period of time can become a risk. A user is the first line of defense for his/her own account, and if the user is not present to notice errors or anomalies, an attacker could use a user's account without being detected. The SHIP NPR website will implement the required **Inactivity Suspension** specification. **User accounts that are not used for one-hundred eighty (180) days will be automatically suspended**. Similar to the "maximum lifetime" rule described earlier, users who attempt to login after a 180 day absence will be required to use the "Forgot Password" link on the SHIP NPR homepage to reset their password. **Note that account suspension DOES NOT delete user accounts**.

## Account Management and Automation

- **How to Change Your Password:** As noted above, the SHIP NPR website has implemented functions to support account security. To support these new security features, we have added a new "**Change My Password**" link within the existing "Edit My Profile" screen. The "Change My Password" link allows you to change your password quickly without having to use the longer "Forgot Password" process.

- **How to Edit Your Email Address:** Additionally, the "Edit My Profile" screen has a new "**Edit My Email**" link that you can use to change the email address associated with your SHIP NPR account. This allows you to change your SHIP NPR user name (their email address) without having to call to SHIP NPR help desk. To use this link correctly, you must be able to access your new email account since the SHIP NPR website will send you a confirmation email at the new email address to verify the change. You will be able to either accept or reject the email change request by clicking on the corresponding links in the confirmation email. Clicking on the "Accept" link will change the e-mail address that is affiliated with your SHIP NPR account. Clicking on the "Reject" link will cancel the email change request. If you do not accept or reject the email change request, you will still be able to log in with your old email address and a valid password.