

## Online Services Customer Portal PASSWORD CHANGE INSTRUCTIONS

<https://portal.pw.utc.com>

Passwords are an important aspect of computer security – they are the keys you use to access your Pratt & Whitney Online Services account. We are implementing a new policy that requires you to change your password every 90 days. A week before your password is scheduled to expire the following screen will appear when you log into the portal:

### Frequently Asked Questions:

#### How do I change my password?

As shown in the dialog box on the right,

- Enter your old password.
- Enter a new password. See the hints below to ensure a “strong” password.
- Re-enter your new password.
- Select the **Change Password** button at the bottom of the dialog box.

If you are unable to change your password, please contact [gppwurequests@pw.utc.com](mailto:gppwurequests@pw.utc.com).

#### How often do I have to change my password?

You must change your password every 90 days.

**What if my account is locked?** After 90 days of inactivity, your account will be disabled (as shown in dialog box below).



You may request a new password by selecting the **Forgot Password** link on the login page. After 365 days of inactivity, you will be removed from our user registration system and will not be able to access the Online Services customer portal.

#### What is a strong password?

A password is less likely to be compromised if it is changed regularly. Your password should be difficult for someone else to guess but easy for you to remember (and type!).

Strong passwords consist of a series of upper and lowercase letters, numbers, and special characters. Typically, the longer the password the stronger it is. Your password should not be easily tied back to the user such as: user ID, given name, social security number, telephone, employee number, phone or office numbers, address, nicknames or family names, pet names, birth date, license plate number, etc.

#### Rules for a strong password:

- Password must contain at least 6 characters with no more than 2 repeating characters
- Password maybe be any combination of uppercase and lowercase letters or digits, punctuation, and non-printable characters
- Passwords are recommended but NOT REQUIRED to be alphanumeric (including both alphabetic and numeric characters)
- Passwords may not be the same as common dictionary words or your login ID
- Passwords may not be reused within a 180 day period

It's best to try to keep your passwords in your head: don't write your passwords down on sticky notes near your computer or store on your computer unless they're encrypted. Don't keep a hard copy file folder of your passwords. Don't give your passwords to anyone. Recent news stories have highlighted how easily people will reveal their passwords, even to complete strangers. Human error continues to be the number one reason that sites are cracked, so be smart and don't share your passwords with anyone.

