

Information Technology Quarterly

Password Policy Implementation

As of **February 5, 2008**, users are now required to change their workstation password to a new “strong” password when their password expires. This new password must meet the following requirements:

- All passwords must contain characters from three of the following four categories:
 - Uppercase English alphabet characters (A through Z)
 - Lowercase English alphabet characters (a through z)
 - Arabic numerals (0 through 9)
 - Special characters such as !\$,#,%).
- The password length must also be at least six characters and must be different from the previous password.

As an additional security measure, users will be required to change their password every 45 days and will be prompted 14 days prior to their password expiring. Also, users will not be allowed to change their password multiple times within one day.

Inside This Issue

Password Policy Implementation.....	1
IT 2009/2010 Master Plan Time Line.....	3
Cellular Tips & Tricks.....	3
The Facts Regarding The Do Not Call Registry	4

These new workstation password requirements will then match OakSource password requirements so users will be able to set both to the same passwords.

These new password requirements are designed to offer a high level of protection for sensitive and personal employee and County information. Although the rules

(continued on page 2)

“Treat your password like your toothbrush. Don’t let anybody else use it, and get a new one every 6 months.” ~Clifford Stoll

may seem cumbersome, the complexity of the password system is what protects the security and privacy of our systems. Your unique user name and password combination is the key that allows you to access information that is stored in the County’s systems. The strong password helps to

keep information well protected from hackers, cyber criminals, and other malicious users who may try to steal information. The Federal Trade Commission estimates that as many as nine million Americans have their identities stolen via the Internet each year.

A strong password system requires the use of a random string of characters (letters and numbers). Each character that is added to a password increases the security of the system, so longer passwords are generally more secure. In addition, the more different characters a password contains, the more difficult it will be for someone to guess the password. Computer security experts normally recommend that passwords contain a minimum of eight characters, and that the password be changed on a regular basis.

The work station password requirements are designed to be as simple as they could be, while still offering a high level of security. To make the most of your strong password, try using words or phrases that are easy for you to remember but difficult for others to guess. Try to create a password that you can remember without having to write it down. Here are some ideas to try when you are required to change your password:

- Use names of pets or your favorite TV characters and then add numbers that mean something to them.
- A sentence that you can remember such as “My son Barry is 19 years old.” Take the first letter of each word of the sentence that you created to create a new word. Using this example, the password would be “MsBi19yo”.



The County is dedicated to protecting the security of employee and County information. Although the password rules might seem inconvenient, it would be even more troublesome if employees’ personal or County information was left vulnerable by an easily compromised password system. A strong password supports the County’s ongoing commitment to ensuring the integrity of its electronic information and the safety of its employees.

Instructions for changing your network password can be found on the IT Training Center web site at http://www.oakgov.com/ittrain/assets/docs/xp_workstation_change_password.pdf.

If you have any questions regarding this implementation, please contact the Information Technology Service Center at (248) 858-8812.

Information Technology 2009/2010 Master Plan Time Line



Information Technology has always played an integral role in County operations. The effective use of technology remains the only feasible method of controlling and maintaining vast amounts of information required to efficiently and effectively operate the County.

The Information Technology staff takes significant pride in the Department's accomplishments and continues to strive towards the most effective solutions to meet the County's business missions, goals, and objectives. The overall goal of the Master Planning process is to develop a clear picture of how Information Technology's resources will support the County's short and long-term information needs.

The Information Technology **2009/2010 Master Plan** time line has been published. At your convenience, please review the informational memo, available under the link entitled **2009/10 Master Plan** on the Project Management Office web site at <http://www.oakgov.com/pmo/>.

If you have any questions, please contact Janette McKenna, Information Technology, at (248) 858-0893.

Cellular Tips & Tricks

by Gloria Logan, Information Technology, Internal Services Division

Receiving Cellular Tower Updates

Periodically, wireless providers update their cellular towers to provide better coverage and reception. In order to ensure the best performance from your wireless device, it is necessary to follow the instructions below. This will enable your device to receive the latest updates that have been made to the cellular towers.



All Models:

Your device should be powered off for 30 seconds on a weekly basis.

(continued on page 4)

Verizon:

Additionally, you should perform the following steps to ensure that you are receiving updated signals from all towers in the area. It is important to follow these steps if you will be traveling out of your local area. This will ensure that you receive the best reception and coverage by picking up tower signals in the area you are traveling to.

1. Press ***228**.
2. Press **Send**.
3. Select option **2**.
4. End the call.



Stopping Spam Messages From Your Phone

If you are receiving unwanted text messages:

1. From the unwanted message, select **Reply**.
2. Type **unsubscribe**.
3. Send the message.

If you continue to receive unwanted messages, submit the message number to the IT Service Center via an incident (<http://sc.oakgov.com>) or by calling 248-858-8812 so this information can be sent to the carrier.

Service Issues

If you are having service issues turn your device off and back on. If the issue persists you can try removing your battery while the unit is on. If the problem is not resolved a Service Center incident should be created.

The Facts Regarding The Do Not Call Registry

by Gloria Logan, Information Technology, Internal Services Division

The following is an example of a false email that is being circulated on the internet:

JUST A REMINDER... 31 days from today, cell phone numbers are being released to telemarketing companies and you will start to receive sales calls. YOU WILL BE CHARGED FOR THESE CALLS.

To prevent this, call the following number from your cell phone: 888-382-1222. It is the national DO NOT CALL list. It will only take a minute of your time. (continued on page 5)

It blocks your number for five (5) Years. Pass this on to all your friends.

The Facts Are:

There is not a deadline to list a phone number with the Do Not Call Registry. Contrary to previous statements, the FTC announced in October 2007 that Registry entries will not expire after five years. Those who signed up when the registry went into effect in June 2003 will not have to register again in 2008. Cellular users can choose to register their cell numbers with the national Registry. Users should note that doing so provides only a small additional measure of protection, as FCC regulations are all ready in place to block the bulk of telemarketing calls to cell phones.

You can verify your registration by going to <http://www.donotcall.gov>.

1. Click the **Verify A Registration** button.
2. Enter your **phone number** and the **email address** you used when you originally submitted your request.
3. Click the **Submit** button.
4. Confirm your information and click the **Verify** button.
5. You will receive an email verifying whether or not you are registered.
6. If you are not registered, click the **Register A Phone Number** button and enter your phone number and email address.
7. You will receive an email to verify registration.

Editor:

Danielle Randall

Contributing Author:

Gloria Logan

Published by:

*Oakland County
Department of
Information Technology*

**1200 North Telegraph Road
Pontiac, Michigan
48341-0421
Phone: (248) 858-0810**

www.oakgov.com/infotech



The Do Not Call registry does not prevent all unwanted calls. It does not cover the following:

- Calls from organizations with which you have established a business relationship.
- Calls for which you have given prior written permission.
- Calls which are not commercial or do not include unsolicited advertisements.
- Calls by or on behalf of tax-exempt non-profit organizations.

There is also concern that the 411 cell phone directory which is being compiled will be used by telemarketers for solicitations. This should not be an issue, as numbers will only be included in the directory if you choose to **opt in**. If a cell phone subscriber does nothing, their number will not be listed in the directory. Since not all cell phone numbers are automatically included, it is unlikely that telemarketers will use the 411 directory.