# Appendix 7: All Technology Policy

macc
CommonWealth

COLLABORATIVE SOLUTIONS FOR
ADMINISTRATIVE CHALLENGES

# MCW Technology Policy

## Introduction

This policy is binding on all staff of MACC CommonWealth (MCW) members. Your use of MCW's computer networks and resources comprises your consent to abide by all terms of this policy. Failure to abide by this policy's terms may result in the loss of your access to MCW technology systems. Your organization may also have additional standards that pertain to your use of agency technology systems as well as additional consequences for failing to meet this policy's provisions.

## General standards

MCW technology systems are provided to help your organization conduct agency business. Your use of technology equipment must be consistent with your agency's activities, operating norms and policies. MCW technology, including e-mail and internet access may *never* be used for the following purposes:

- activities that are illegal or of questionable legality (including violations or potential violations of copyright law), that provide commercial or other private benefit to the user, that attempt to advance or solicit for religious causes, or that support or oppose political candidates, parties or campaigns.
- to send messages, pictures, or files, or to access pictures, files or web sites that are illegal, pornographic, obscene, insulting, racist, discriminatory or offensive
- to maliciously destroy or damage information, attempt unauthorized access on any system, or otherwise disrupt MCW or other parties' technology systems in any way.

Users of MCW electronic mail system should create messages carefully and maintain a professional standard of courtesy in both internal and external messages.

Bulk e-mail to external e-mail recipients (that is, recipients outside the MACC CommonWealth system) is not supported in MCW's environment. Bulk e-mail is defined as sending the same message to 100 or more external recipients, whether in the same e-mail or spread across multiple e-mails.

All information transmitted by, received from, or stored in MCW computer system is property of one or more of MACC CommonWealth's member agencies. Users of MCW systems have no expectation of privacy—we have an unrestricted right to monitor and review any user's activities or files at any time.

## Protection of technology systems

MACC CommonWealth makes substantial investments in maintaining its technology systems. The following standards are designed to protect the safety, legal operations and availability of our systems:

- all equipment must be treated carefully, including securing laptops in offices (users of laptop are also responsible for their protection when transporting the laptop or using it outside the office)

- software can loaded only under the control of MCW technology management
- only MCW technology staff may set up and install equipment, as well as attach or configure modems or other communications equipment
- no personally owned equipment may be attached to MCW systems except as authorized by MCW technology management.

**Security and access controls**

Because MCW systems contain confidential and other sensitive information, including information protect by federal law, all users must abide by system security and access controls. Users must be careful to:

- protect the confidentiality of all passwords—you are accountable for all activities performed under your user account
- protect client confidentiality as required by law or your agency's policy
- exercise extreme care when accessing or retaining information on portable media, including laptop hard drives, smartphones, disks, CD-ROM and DVD media, "flash" drives.

System users may not

- use or attempt to use another person's user name or password (with or without that user's permission), or attempt to learn another user's password
- display or keep passwords where they can be viewed by others
- attempt to view information for which they are not authorized or for which they have no business purpose.

**Guide to Passwords:**

Effective August 1, 2008, MACC CommonWealth has the following requirements for network passwords:

- must be at least six characters long
- must include one or more upper-case letters, one or more lower-case letters, and one or more numbers
- will change every 60 days (the system will enforce this automatically
- may not repeat any of the three previous passwords

We are moving to "stronger" passwords to protect the confidentiality of our information. Our previous standard was not strong enough to provide adequate protection given the confidential nature of so much of our information (including client data protected by both state and federal law).

**Tips for making this easier**

Here's a simple approach you can use to select a new password that complies with these requirements:

- Select an easy-to-remember proper noun (that is, the name of a person, place, etc.) that is at least five letters long. This will meet the requirement to have both upper-case and lower-case letters in your password.

- Add a numeral "1" to the end of this password. When that password expires, add a numeral "2." You can change this to "3" and then "4" to comply with the rule that does not permit using any of the last three passwords. On your fifth change, you can either go back to "5" or continuing increasing the number.

For example, if you had a son named "Robert," you could use "Robert1" as your initial password, followed by "Robert2" when the first password expires in 90 days. When the second password expires, you could use "Robert3" and so on.

*Do not use your own name as the basis for your new password*. A password that can be guessed at by others is as bad as no password at all.

**Remember: "three strikes and you're out"**

When logging in to the network, be aware that:

- Passwords are case sensitive. If you mix up the upper-case and lower-case letters, or accidentally have the caps lock key on, the system will not log you in.
- If you try logging in unsuccessfully three times in a row, the system will lock your account. You will need to contact our help desk during normal business hours to get your account unlocked.

If you are unsuccessful logging on the first time, *make sure the caps lock key is off and type your password slowly and carefully the second time*. It is easy to get to "three strikes" by moving too fast after the first failure to log in—be careful with your second and third tries!