



QualityIT™

Security Awareness Policy & Practice

Every employee in every role contributes to the safety, security, and regulatory compliance of an organization

Every employee is
expected to apply
prudent security
judgment when
conducting company
business

Where the security of
an organization is
concerned,
personal vigilance is
required

Never share your
company password
with anyone — even
ops personnel —
without first obtaining
authorization from
your direct manager

Never leave your
workstation logged in

Click `ctl-alt-del` and
select “Log Off” any
time you leave your
chair

Never write your
company password
down anywhere

Instead obtain a secure
password storage
application from a
trusted source

Report any suspicious individuals to the proper authorities immediately that are observed in or around the workplace

Internet searches or
visiting unauthorized
websites using
company computers
could cause serious
problems

Obtain authorization

Obtain authorization
before using your
company computer for
any personal business

If you think your
computer is acting
strangely or you
suspect your computer
may be compromised,
notify the proper
authorities immediately

Delay in reporting a suspected problem is more serious than having introduced the problem

Never hesitate to report
a personal
misjudgment to the
proper authorities

Never open any
attachment or email
from an unknown
source

Never launch email from
anyone you don't know

Should you receive
unexpected mail from
someone outside the
company that you
know, check by phone
with them
before opening it

Notify company
authorities if you are
receiving SPAM or
solicitation messages
to your inbox

Don't store company
information on your
laptop computer

Obtain an authorized
remote access account
for work at home

Never allow anyone to
“piggyback” you
through a secure door

Report suspicious
behavior by anyone
you observe in the
workplace
to the proper
authorities

Suspend activity on your
computer anytime someone
visits you at your cube who
does not need specifically
need to see your work

Never take your
company laptop or
handheld device on
vacation

If you have to travel for work, never leave your devices unattended in a conference or hotel room

Never install any
application on
company computers
or devices that are not
explicitly authorized
for your work

Engage unattended
guests in conversation
and stay with them
until their sponsor has
returned

Be aware of what
constitutes sensitive
information in your
work

Don't provide any more
information than is
necessary in email
and voice mail
messages

Security depends on
common sense and
personal vigilance

Our security is in your
hands!

Vulnerability

Policy & Practice

(derived from Michael Howard's Tips)

http://blogs.msdn.com/michael_howard/

Accept ownership for
your machine.

You are the only one in
charge so you are the
only one responsible!

Check your User List:

Investigate anyone
other than you who has
Admin Right to the
machine

Use strong passwords

Mix of letters, numbers
and symbols,
preferably avoiding
common words

Make sure the firewall
is on!

Make Deliberate
Settings Choices

Prohibit Installation of
Active Objects

Execute 1st of month:

Purge unknown cookies

Run:

Rootkit Revealer Utility

Port Reporter Utility

Anti-Spyware Utility

Security Baseline Utility

Snapshot Task Mgr.

Get familiar with
common services
running and typical
performance metrics.

Investigate anomalies

Rename all share ware
anti-virus/spyware
executables

Knowing the common
name allows malware
to overwrite it or avoid
it

Install and use more
than one Anti-Virus
software (ie. MS,
Norton, AVG)

Consider Prevention
Software (ie. PrevX)

Install and use more
than one Anti-Virus
software

Consider Prevention
Software

Enable Auto Updates and Notifications

For OS

For Office & other Apps

For Prevention Software

For Anti-Virus

For Anti-Spyware

Hit Stand By when you
leave your computer

(Computers not running
can't be hijacked)



QualityIT™

Contact me for any
questions or
suggestions for
improvement

barbis@qualityit.net

QualityIT™

Be vigilant Stay Safe

Resource site

securityprocessprofessional.com

