Protecting Your Workplace: Guidance on Physical and Cyber Security, and Reporting Suspicious Behavior, Activity and Cyber Incidents

CYBER SECURITY GUIDANCE

Employees

- Make your passwords complex. Use a combination of numbers, symbols and letters (uppercase and lowercase).
- Change your passwords regularly (every 45 to 90 days).
- Do NOT give any of your usernames, passwords or other computer/Web site access codes to anyone.
- Do NOT open e-mails or attachments from strangers.
- Do NOT install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department.
- Make electronic and physical back-ups or copies of all your most important work.
- Report all suspicious or unusual problems with your computer to your IT department.

Management & IT Department

- Implement Defense-in-Depth: a layered defense strategy that includes technical, organization and operation controls.
- Establish clear policies and procedures for employee use of your organization's information technologies.
- Implement Technical Defenses: firewalls, intrusion detection systems and Internet content filtering.
- Update you anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer's default passwords on all of your software.
- Monitor, log and analyze successful and attempted intrusions to your systems and networks.

REPORT SUSPICIOUS CYBER INCIDENTS

System Failure of Disruption

Has your system's or Web site's availability been disrupted? Are your employees, customers, suppliers or partners unable to access your system or Web site? Has your service been denied to its users?

Suspicious Questioning

Are you aware of anyone attempting to gain information in person, by phone, mail, e-mail, etc., regarding the configuration and/or cyber-security posture of your Web site, network, software or hardware?

Unauthorized Access

Are you aware of anyone attempting (either failed or successful) to gain unauthorized access to your system or its data?

Unauthorized Changes or Additions

Has anyone made unauthorized changes or additions to your system's hardware, firmware or software characteristics without your IT department's knowledge, instruction or consent?

Utica National Insurance Group • Utica Mutual Insurance Company and its affiliated companies, New Hartford, NY 13413 • www.uticanational.com

Form 5-R-612 Ed. 02-2010

Suspicious E-mails
Are you aware of anyone in your organization receiving suspicious e-mails that include unsolicited attachments and/or requests for sensitive personal or organization information?

Unauthorized Use
Are unauthorized parties using your system for the processing or storage of data? Are former employees, customers, suppliers or partners still using your system?

PHYSICAL SECURITY GUIDANCE

Employees & Management

- Monitor and control who enters your workplace: current employees, former employees, and commercial delivery and service personnel.
- Check identification and ask individuals to identify the purpose of their visit to your workplace.
- Report broken doors, windows and locks to your organization's or building's security personnel as soon as possible.
- Make back-ups or copies of sensitive and critical information and databases.
- Store, lock and inventory your organization's keys, access cards, uniforms, badges and vehicles.
- Monitor and report suspicious activity in or near your facility's entry/exit points, loading docks, parking areas, garages and immediate vicinity.
- Report suspicious-looking packages to your local police. DO NOT OPEN or TOUCH.
- Shred or destroy all documents containing sensitive personal or organizational information that is no longer needed.
- Keep an inventory of your most critical equipment, hardware and software.
- Store and lock your personal items such as wallets, pursues and identification when not in use.

REPORT SUSPICIOUS BEHAVIOR AND ACTIVITY

Surveillance
Are you aware of anyone recording or monitoring activities, taking notes, using cameras, maps, binoculars, etc., near a key facility?

Deploying Assets
Have you observed abandoned vehicles, stockpiling of suspicious materials or persons being deployed near a key facility?

Suspicious Persons

Are you aware of anyone who does not appear to belong in the workplace, neighborhood, business establishment or near a key facility?

Suspicious Questioning
Are you aware of anyone attempting to gain information in person, by phone, mail, e-mail, etc., regarding a key facility or its personnel?

Tests of Security
Are you aware of any attempts to penetrate or test physical security or procedures at a key facility?

Acquiring Supplies
Are you aware of anyone attempting to improperly acquire explosives, weapons, ammunition, dangerous chemicals, uniforms, badges, flight manuals, access cards or identification for a key facility, or attempting to legally obtain items under suspicious circumstances that could be used in a terrorist act?

Dry Runs
Have you observed any behavior that appears to be a preparation for terrorist activity, such as mapping out routes, playing out scenarios with others, monitoring key facilities, timing traffic lights or traffic flow, or other suspicious activities?

For more information on physical and cyber security countermeasures, visit www.US-CERT.gov, a divisional Web site of the U.S. Department of Homeland Security.

Utica National Insurance Group • Utica Mutual Insurance Company and its affiliated companies, New Hartford, NY 13413 • www.uticanational.com

