# Computer Services Acceptable Use Guidelines

## Acceptable use

Employees using the Internet are representing the organization. Employees are responsible for ensuring that the internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using the Web browsers to obtain business information from Commercial Web sites
- Accessing databases for information as needed
- Using e-mail for business

## Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the organization, or nonproductive. Examples of unacceptable use are:

- Sending and forwarding chain e-mail, i.e. messages containing instructions to forward the message to others.
- Broadcasting e-mail, i.e. sending the same message to more than 10 recipients or more than one distribution list.
- Forwarding any e-mail containing an attachment with an EXE, VBX, or SRC extension (as these file types are frequently used to carry computer virus attacks).

## Downloads

File downloads from the Internet are not permitted unless specifically authorized in writing by the IS manager.

## Employee responsibilities

An employee who uses the Internet or Internet e-mail shall:

a. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
b. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
c. Not transmit copyrighted materials without permission
d. Know and abide by all applicable policies dealing with security and confidentiality of organization records.

# Computer viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

## Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure.
- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

### Employee responsibilities

These directives apply to all employees:

e. Employees shall not knowingly introduce a computer virus into organization computers.
f. Employees shall not load diskettes of unknown origin.
g. Incoming diskettes shall be scanned for viruses before they are read.
h. Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IS manager.
i. Employees should not open e-mail attachments from unknown sources unless the receipt of such e-mails are a part of their normal duties
j. Employees should never open an e-mail attachment or forward an e-mail containing an attachment that has a file name with an EXE, VBX, or SRC file extension.

## Physical security

It is organization policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

### Employee responsibilities

The directives below apply to all employees:

a. Diskettes should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
b. Diskettes should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
c. Critical computer equipment, e.g. file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
d. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
e. Do not share your network or e-mail password with others. In the event that you believe your passwords are known by others, contact Computer Services.

_____ _____

Employee signature Date