

# ACCEPTABLE INTERNET PRACTICES

(provided by ELM Computer Systems Inc.)

Given that use of the internet is universal in today's corporate environment, ELM Computer Systems Inc. ([www.elmcomputers.com](http://www.elmcomputers.com)) is making available this standard procedure on Acceptable Internet Practices by employees using the Internet on behalf of their employers. We encourage you to modify this document as necessary for your own purposes.

## 1 – Security

### A – Intrusion protection

- i – Security measures (antivirus, antispymware, spam filter, firewall, etc) must be installed as necessary on all systems with internet access.
- ii – Security measures must be regularly updated, with full system scans to be performed after each update (or at a reasonably frequent interval).
- iii – Department heads and system administrator must be informed upon discovery of any security breach and appropriate measures taken to secure all affected systems.

### B – Email and email attachments

- i – Unsolicited email must be considered as potential threats, regardless of the source, until it has been certified virus free by the sender, department head or system administrator.
- ii – All email confirmed to be a threat must be immediately removed from the system.
- iii – No attachment may be opened unless it has been requested from and sent by a known and reliable source except with the approval of the department head.
- iv – Unsolicited email attachments may not be opened under any circumstance, regardless of the source, until its legitimacy can be verified by sender, department head or system administrator.

### C – Software

- i – Under no condition is any item available on the internet to be purchased, downloaded, or installed unless prior approval has been given by the department head or system administrator.

### D – Confidentiality

- i – Internet account and access information (account names, passwords, IP addresses, etc.) must be treated with confidentiality and may not be transmitted to any person not an employee of, or approved by the organization unless approved by the department head.
- ii – All personal access information is to be removed upon relocation or termination of employment.
- iii – Personal access information may not be transferred between employees within the organization unless approved by the respective department heads.
- iv – No information or file belonging to the organization is to be transmitted over the internet, except to approved recipients, unless approved by the department head.

2 – Fair Use

A – Internet access is provided primarily for the communication requirements of the organization and is intended primarily to be of benefit to the organization.

i – Personal use of internet resources:

- a – Must not place data or resources belonging to the organization at risk.
- b – Must not interfere or conflict with employees' performance of their duties.
- c – Must not jeopardize integrity of the organization and its computer systems.
- d – Must not negate the benefit of internet to the organization.

ii – Files and/or data must not be transmitted over the internet unless approved by the department head. Operating system updates, updates to installed applications, and security updates are excepted from this restriction if approved by the department head or system administrator.

3 – Oversight

A – Internet use by employees is to be monitored by department heads with ultimate oversight resting with the system administrator of the organization

B – Department heads and/or the system administrator may request and/or review all internet access, email, and internet activity logs on systems under their authority.

C – Department heads and/or the system administrator may request and/or place restrictions on systems/individuals under their authority if necessary.

4 – Consequences of improper use may include any or (progressively) all of the following:

- A – Warning.
- B – Monitoring of internet usage.
- C – Reduction, or removal of email privileges.
- D – Reduction, or removal of internet privileges.
- E – Reduction, or removal of computer privileges.
- F – Termination.

System Administrator: \_\_\_\_\_ Date: \_\_\_\_\_  
(or representative)

Employee/Consultant: \_\_\_\_\_ Date: \_\_\_\_\_