

ACCEPTABLE COMPUTER PRACTICES

(provided by ELM Computer Systems Inc.)

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

1 – Security

A – User names, account names, passwords, access codes and any other data enabling access to resources belonging to the organization are the property of the organization and are strictly confidential. This information is entrusted to employees of the organization for the sole purpose of enabling them to perform their required tasks. Under no circumstance is this information to be distributed to any other party (within or without the organization) without the express consent of the department head and system administrator.

B – No software of any nature may be installed on any computer owned by the organization without the express consent of the department head and system administrator, regardless of its perceived benefit to the organization, with the following exceptions:

i – Software may be installed on computers not owned by the organization if the system administrator can be satisfied that said software does not conflict with the interests of the organization or expose the property of the organization to risk.

ii – Under no circumstances is any form of software capable of negating organizational security settings to be installed on any computer used on behalf of the organization. This includes any variant of Peer-to-Peer software connecting a computer used on behalf of the organization to a computer with no association to the organization. A computer will be disqualified for use on behalf of the organization if any such software has been installed on it and has not been removed to the satisfaction of the system administrator.

2 – Fair Use

A – It is understood that computer systems used on behalf of the organization are resources belonging to the organization and are to be used in the best interests of the organization.

B – Personal use of any computer system owned by the organization or used on behalf of the organization must comply with the following standards:

i – Material of personal interest may not be accessed outside of personal time.

ii – Material of personal interest may not be accessed on personal time if access conflicts with the interests of the organization or exposes the property of the organization to risk.

iii – Material of personal interest may not be accessed at any time if such behaviour would damage the reputation of the organization.

C – In the event that a computer not owned by the organization is used on its behalf it is understood that:

i – The computer remains the property of its owner but when used on behalf of the organization it is considered a resource owned by the organization and is governed by this policy.

ii – The owner of the computer is required to ensure that the security settings of the computer attain the minimum security requirements of the organization and are adequate to protect the property the organization which it has access to. The system administrator has the right to evaluate system security and require any of the following:

- a – The computer be upgraded to conform to the requirements of the organization.
- b – The computer be given restricted access of resources belonging to the organization.
- c – The computer not be used on behalf of the organization.

3 – 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: _____

ELLM
COMPUTER SYSTEMS INC.