Policy Title: Acceptable Use – Internet Access and E-mail

Date of Approval: October 19, 1999

Policy Number: HUM-001-00018

Lead Role: HRO

Support Role: Manager Info. Serv.

Cross Reference: Next Review Date:

Council File Number: 99-145

Revision Date:

Policy Statement:

This document contains guidelines and procedures governing Internet access and all forms of Internet communication (including but not restricted to e-mail, web-based forms and newsgroup posts).

This policy applies to employees, elected officials and any person authorized to use the Corporation’s resources.

Access Request

Individuals will be granted access to each unique Internet service (e.g. e-mail or web) based on need. It is the responsibility of each Department Head to assess the requirements of staff, and to forward requests via e-mail to the I.S. Manager. The request must include the work-hours the employee is normally permitted to use the network, and the reasons Internet services beyond e-mail may be required if applicable.

Access will be granted only after Corporation approval, and only after receiving signed agreement to this policy and the current standards document.

Scope of this policy

Internet services are provided to conduct official City business only.

The City of Welland retains ownership and exclusive control over the reproduction of Internet communications. The City of Welland reserves the right to log, monitor and review all access and content. The City may at any time filter or otherwise restrict communication to or from the Internet. Access may be controlled for individuals, groups or all users based on specific need and security considerations. These restrictions may include, but are not limited to the following:

- Access limited to approved destinations.
- Access limited by content rating.
- Access denied by specific destination.
- Access rejected for specific (or unverified) sources - such as ‘spam’ junk mail.
No person will employ methods that prevent easy access to communicated information (encryption, password protection, file formats not common to daily City operation, etc.) unless specifically authorized.

Existing policies concerning harassment and inappropriate behavior apply. General legal, ethical and moral standards apply. Software piracy, copyright infringement, the access, transport or storage of offensive or obscene material, hate literature, etc. will not be tolerated.

Because of increased risk and to address other concerns, some general security controls will be tightened. A change that everyone needs to be aware of, is that access to the network will be restricted to the normal hours of work for most employees. If an individual requires additional computer time, their Department Head should contact the I.S. Manager to arrange access.

Responsibility

The Corporation assumes heightened security risk by allowing access to the Internet. To protect corporate assets, certain general computer procedures must be tightened for the equipment and users involved.

Passwords

- Password selection and renewal period will be based on current City standards. A standards document will be available to all users.
- Passwords must remain secret. No password should be written down, disclosed or shared for any reason.
- Unique passwords and user names may be required for different systems for security reasons.
- The City may audit passwords at any time. Accounts not conforming to standards will be disabled pending correction.
- Repeated violations may result in service termination or further action.

Virus protection.

- Virus definition files must be updated frequently, based on a current standards document.
- Unsolicited e-mail attachments must not be opened, even from trusted sources.
- Employees shall not download any executable software (contact I.S. if such files are required).
- I.S. must be notified of potential virus or security threats. Messages received warning of potential virus threat should be forwarded to I.S. for investigation. Many of these warnings are hoaxes.

Access

- Use of City based Internet services by third parties is not allowed unless authorization is received.
- All access to City systems and Internet services must be performed with your own access rights (logged into the system under your name).
- An electronic signature may be required (specified in the current standards document) at the end of each e-mail message or forum posting.
Health & Safety Hum-001-0018

Etiquette

- The Internet has unique rules of appropriate behaviour. For example, typing letters in ALL CAPS is considered impolite (yelling). A style checklist is available on the standards document.

Personal Responsibility

Charges resulting from non-compliance shall be the personal responsibility of the employee. The employee will be responsible for costs and damages sustained by the Corporation or third parties and will be obligated to indemnify the Corporation for any claims.

Enforcement

The City reserves the right to suspend or terminate access of any and all employees at any time. Action may be taken because of external threat or if inappropriate employee use is suspected.

Failure to comply with this policy may result in the loss of Internet privileges, and depending on the severity, disciplinary action up to and including dismissal.

Periodic Review of Policy and Standards

This policy document will be reviewed every two years at a minimum. The Current Internet Use Standards document will be reviewed more frequently. Changes to either document will require a signature confirmation. Internet access will expire unless the new document is signed.