



DRUMHELLER

COUNCIL POLICY



COUNCIL POLICY # C-6-99

DATA SECURITY POLICY

BACKGROUND:

The Freedom of Information and Protection of Privacy Act requires that public bodies take reasonable measure to provide an appropriate level of security for the personal information that is in their custody or under their control (Section 36). The Act also contains a number of exceptions to the right of access to information where the disclosure of that information could reasonably be expected to cause a direct or indirect harm to one of the interests listed in Sections 15 to 28.

PURPOSE:

The municipality relies heavily on the application of information technology for the effective management of its programs. The value of the information, software, hardware, communication systems, mapping applications, etc. must be protected against loss or unauthorized use.

POLICY:

The security policy will:

1. Protect the information resources of the Town against loss or unauthorized use.
2. Comply with the requirements of Freedom of Information and Protection of Privacy Act.

PROCEDURES:

Measures shall be taken to protect information against negligent or unauthorized use, disclosure, modification or destruction as follows:

- 1) Security awareness and training of all employees - the policy shall be part of all new employee orientation.
- 2) Each employee and contractor (third party user) shall sign a confidentiality (non-disclosure) statement.


- 3) Each employee shall ensure that all sensitive information as classified in Schedule A is protected by special handling.
- 4) Removal of sensitive information and valuable assets from the municipality's premises is restricted and requires authorization from the department head.
- 5) Each employee shall secure his/her own computer work station against unauthorized access by the use of passwords in accordance with Schedule B.
- 6) Each employee shall protect the files (hard copy and electronic) in their work area from unauthorized access.
- 7) Each employee shall follow proper operating instructions for their computer and other hardware equipment as specified by the System Administrator to reduce the risk of negligent or deliberate system misuse.
- 8) Computer systems shall be monitored by Department Heads to ensure compliance to policy and standards.
- 9) Electronic and hard copy filing systems shall be monitored by Department Heads to ensure compliance to policy and standards.
- 10) All keys to office doors, filing cabinets, and secured areas are to be assigned to an individual by the Department Heads.
- 11) The combinations to vaults shall only be given to those who require access.
- 12) Incidents affecting security should be reported to Department Heads as quickly as possible for corrective action.

FORMAL DISCIPLINARY PROCESS:


All individuals who do not comply with security procedures and commit security breaches are subject to formal disciplinary action.

Adopted by Council

Date: September 13, 1999



Mayor of Drumheller



Chief Administrative Officer

SCHEDULE A

Sensitive information requires special handling when it is transferred internally or externally. The following method of handling is recommended:

<u>CATEGORY</u>	<u>METHOD OF HANDLING</u>
<u>LOW SENSITIVE INFORMATION</u> (Confidential in nature) <ul style="list-style-type: none">- Payroll Cheques- Resumes- Character References	Sealed envelope addressed to recipient.
<u>HIGH SENSITIVE INFORMATION</u> (If released, cause harm to an individual or third party - mandatory protection) <ul style="list-style-type: none">- Contractual Information- Litigation (Legal opinions)- Medical Records- Law Enforcement- Information relating to tax returns- Financial Information- Land Dealings- Personal Evaluation	Marked confidential on the document. Sealed envelope addressed to the recipient. Envelope to be marked with one of the following: Confidential and Private; To be opened by the addressee only; Personal.

SCHEDULE B

Login ID Passwords

In order to comply with this policy, each employee logging in to the network will require a password to enter the system. This password will be changed every three months by a system prompt requesting a new password. The new password cannot be the same as the previous two words used.

Screen Saver Password Protection

In order to comply with this policy, each employee will use a Microsoft approved system screen saver with password protection enabled. The screen saver must start up within ten minutes of the employee leaving the workstation unattended except in the case of the financial system users where a longer period between start-ups is necessary. Any employee who leaves their workstation running after they have left for the day will have their terminal shut down by the Office Automation Coordinator (OAC) responsible for that area.

Password Protected Files

Any highly sensitive confidential files will be protected by passwords in secured directories. These files include any personnel issues and budget files approved by Council. Once a password is assigned to a file only two people will have access to the password; the creator of the file and the department head. This password must be different from both the creator's login ID password and the department head's login ID password. These passwords will be stored in a secure place within the department head's office.