MUNICIPAL DISTRICT
BONNYVILLE NO. 87

POLICY

Systems and Data Security Policy

2A.014

Section: **2.0 General Government and Administrative Services**
- **A. Governance**

Authority: **Chief Administrative Officer**

Statement

The Municipal District of Bonnyville (M.D.) promotes computer usage that assists users in performing their duties for the municipality. Every user is responsible for adhering to this policy and for following the procedures related to this policy.

All data created or stored on the M.D.'s Information Systems is the absolute property of the M.D. Security procedures shall be implemented to ensure the confidentiality, integrity and availability of such data.

The M.D. uses software only in compliance with license agreements. No unlicensed software shall be installed on Municipality Information Systems.

Purpose

(1) The Municipal Information Systems include, but are not limited to, electronic mail (e-mail) and the Internet. The purpose of these systems is to provide efficient and effective means of internal and external communications, to improve work productivity.

(2) This policy and its related procedures:
   (a) Address access to and the disclosure of information from the Information Systems.
   (b) Guides users in the performance of their duties.
   (c) Serves to delineate acceptable uses of the Information Systems by users.

(3) Further, this policy seeks to ensure that user guidelines are consistent with M.D. policies, all applicable laws, and the individual user's job responsibilities.

(4) The M.D. promotes computer, Internet and e-mail use that enables employees to perform municipal missions and encourages its employees to develop computer, Internet and e-mail skills and knowledge.

(5) It is expected that employees will use the Internet and e-mail:
   (a) To access scientific, technical, and other information on work-related topics to increase job knowledge.
   (b) To communicate with others as relevant to their work for the municipality.
   (c) For incidental and occasional personal use within the allowable bounds.

Definitions

For the purposes of this policy, status employment definitions are as follows:

(1) "Information Systems" is all technical resources that are owned or leased by the M.D. that are used on or accessed from municipal premises or that are used for municipal business; including but not limited to municipal owned or leased equipment, software, facilities, desk phones, cell phones, computers, internet addresses, domain names, e-mail services registered to or provided by the municipality, and any municipal paid accounts, subscriptions or other technical services.

(2) “Users” are all full or part-time employees of the M.D., elected officials, volunteers and contractors who are authorized by the Chief Administrative Officer (CAO) to use Municipal Information Systems.

(3) “Remote Users” are any users who access the M.D. Municipal Information Systems from a network not operated by the M.D. Information Technology department.

Procedure

Use of Information Systems

(1) The M.D. provides Information Systems to users for the purpose of performing their duties for the municipality in an effective, ethical, and lawful manner. These systems, like other municipal assets, should be used for the benefit of the municipality.

(2) All use should be congruent with the municipal governance, corporate policies, and local law.

(3) The municipality reserves the right to monitor and/or log all network activity, with or without notice, including all web site communications. Users should have no expectations of privacy in the use of these resources. Use of Information Systems in violation of this, or other municipal policies, is prohibited and may lead to disciplinary action, up to and including termination.

(4) Incidental and occasional personal use of Municipal Information Systems is permitted. This would include use for education purposes, personal development, work for community groups, etc. Any personal use of Municipal Information Systems must be done outside of normal working hours, provided there are no additional costs to the municipality and that all other provisions of this policy are adhered to. For the purpose of this paragraph, lunch break and coffee breaks are not deemed “Normal Working Hours”. At no time can any of the Municipal Information Systems be used for personal gain. Consumable materials and other direct costs will be on a user pay basis.

(5) The Information Technology department reserves the right, without delay, to revoke the system access for those responsible where it appears there is an immediate threat to security.

(6) Any municipal staff or third party allowed access to M.D. systems must agree to and sign the M.D. Systems and Data Security Policy Statement *(Attachment A)* which confirms their awareness and acceptance of this policy and associated procedures. Any remote users must also agree to and sign the Remote Access Agreement *(Attachment B)*.

Policy Review

Within five (5) years from date adopted / amended / reviewed.

For administrative use only:

Previous Policy Number: (prior to July 24, 2019)	10.12.35
Related Documentation: (plans, bylaws, policies, procedures, etc.)	Attachment A: Systems and Data Security Policy Statement Attachment B: Remote Access Agreement

Systems and Data Security Policy Statement

The Municipal District of Bonnyville (M.D.) Systems and Data Security Policy requires that anyone provided access to the municipality's Information Systems is to complete and sign this form.

I acknowledge that I have read and agree to comply with the following M.D. policies and procedures:

(1) Systems and Data Security Policy

Name: ______________________________________

Department: __________________________________

Signature: ____________________________________ Date:_____/_____/_____

Anyone who accesses M.D. computer systems should be aware that interference with electronically stored data is a criminal offence, according to the Canadian Criminal Code, as amended. The following includes summaries of the relevant Criminal Code sections:

Section 430 (1.1) "Mischief in Relation to Data":
"Anyone who willfully destroys or alters data; renders data meaningless, useless, inoperative or ineffective; obstructs, interrupts or interferes with the lawful use of data; or obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access... is guilty of an offence and liable to imprisonment for a term not exceeding ten years."

Section 342.1 (1) "Unauthorized Use of Computer"
"Anyone who, fraudulently (a) obtains, directly or indirectly, any computer service, (b) intercepts or causes to be intercepted, any function of a computer system, (c) uses or causes to be used, a computer system with intent to commit an offence under (a) or (b) or an under section 430; is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years."

Remote Access Agreement

Purpose and Scope

I understand I am being granted permission to remotely access the Municipal District of Bonnyville (M.D.) Information Technology (IT) system as a remote user and that my use of this access may be monitored by the municipality for compliance with this Agreement and the M.D. Systems and Data Security Policy. I understand that my failure to comply with IT security policies may result in termination of my remote access privileges and/or disciplinary action, or in the case of contractor access, termination of contracts.

This agreement applies to all M.D. employees, contractors, vendors and agents with a municipal-owned or personally-owned computer or devices used to connect to the municipalities network. This policy applies to remote access connections used to do work on behalf of the M.D., including but not limited to reading or sending email and viewing intranet resources. Remote access implementations that are covered by this policy include, but are not limited to VPN, SSH, and RDP connections, etc.

Protection of Data

I acknowledge my responsibility to ensure the confidentiality, integrity, and availability of all forms of Government information in accordance with Alberta Freedom of Information and Protection of Privacy Act, M.D. Systems and Data Security Policy and any applicable laws, in a manner consistent with its sensitivity. I accept my responsibility to provide reasonable physical security for all municipal resources issued to provide this remote access. I agree to implement and maintain, as directed, the following mandatory countermeasures on equipment used to process municipal information:

(1) Configure computers to not “remember” municipal access passwords.

(2) Do not share or reveal municipal usernames and passwords with anyone (including family members) to prevent unauthorized access to municipal IT systems and data.

(3) Install and configure to automatically update (at least bi-monthly) and run anti-virus software on personally owned equipment used for remote access.

(4) Install and update (at least monthly) security related patches on personally owned devices that can be patched.

(5) Close browser when finished with remote access needs for personally owned equipment.

(6) Do not save Government information and applications to the hard drive of the remote access computer unless specified below.

(7) Agree to comply with regularly scheduled maintenance requirements for municipal resources. (municipal owned equipment will be brought in for maintenance.)

(8) Never configure remote access computers as servers (e.g. web servers, private e-mail servers, File Transfer Protocol servers (ftp)). (Do not install software on municipal computers.)

(9) Install and use password-protected screensavers when idle for 15 minutes or more.

(10) Remote access users will maintain hardware and software as required.

(11) Remote access users will abide by the license agreements for all municipality-furnished software.

(12) Do not use non-municipal email accounts (I.e., Hotmail, Yahoo, Gmail), or other external resources to conduct municipal business, thereby ensuring that official business is never confused with personal business.

I **will not** alter the configuration of government equipment unless authorized in writing to do so. I will protect municipality-owned/furnished resources and submit the equipment for periodic maintenance or annually as required.

Incidents

I also acknowledge the possibility, however small, that such information could potentially be viewed or downloaded by others than myself as a result of my remote access. I fully understand that it is my duty to exercise due care in protecting this information and to immediately report an unauthorized disclosure or compromise to my supervisor, the Chief Administrative Officer and Manager of IT so that appropriate procedures may be initiated. I further understand that, if required legally, by and after proper coordination (properly executed warrants etc.) with law enforcement authorities, the Government may temporarily seize the device used to gain remote access for the purposes of forensic examination and sanitizing of compromised information. Additionally, during this process I understand there exists a risk that system files and programs may be erased or damaged, or that unintentional damage may occur to the computer hard drive. I hereby waive any and all claims against the M.D., and individual officers, employees, agents and contractors thereof, arising out of necessary security procedures and actions with respect to personally-owned IT equipment and any such damage to, or erasures of personal data.

I acknowledge that the municipal IT department does not provide any assistance, support or advice respecting any problems with the remote access account holder's personal equipment or internet connection.

I acknowledge my responsibilities as described and certify I have received appropriate training and guidance to ensure the confidentiality, integrity, and availability of all forms of Government information in accordance with all policies and in a manner consistent with its sensitivity.

User's Printed Name/Signature:

__________________________/__________________________ Date______________________

General Manager Approval (Printed Name/Signature):

__________________________/__________________________ Date______________________

(For IT Use only)

Remote Access Authorization:
Remote access, as described in this agreement, is Approved _____ Disapproved _____

Printed Name/Signature, Information Technology Manager:

__________________________/__________________________ Date______________________