Policy Number:	**PRIV-1-6**
Policy Name:	**Information Handling and Security**
Issued:	**02.2025**
Revised:	
Applies to:	**E**

PREFACE

McMan South Region (referred to as "McMan") has business, ethical and legal responsibilities to protect all forms of personal information and personal employee information in its custody and/or control.

The purpose of this policy is to outline administrative, technical, and physical safeguards in place at McMan to protect personal information against unauthorized access, collection, use, disclosure, or destruction.

This document should be read in conjunction with McMan's Privacy Charter and all the related policies and procedures referenced therein.

POLICY

Administrative Safeguards

1. McMan ensures that policies and procedures to facilitate the safeguarding of confidential information in its custody or control are developed and maintained.
2. Privacy Policies and procedures are reviewed as required as per Policy Committee Terms of Reference. Substantive revisions and/or amendments are approved in writing.
3. The need for confidentiality and security of personal information is addressed as part of the conditions of employment for McMan employees, beginning with the recruitment stage, and included as part of job descriptions and contracts. All employees are aware of, and appropriately trained with regard to, policies and procedures for safeguarding information.
4. All McMan employees that collect, use, disclose or have access to confidential information as part of the performance of their duties for McMan sign a Confidentiality Agreement (Appendix 4).
5. Utilizing a system of access as required by role, only the least amount of information necessary for the intended purpose shall be used or disclosed, and only to employees with a need to know. If the intended purpose can be accomplished without use or disclosure of identifying information, then the information is made anonymous.
6. Before implementing proposed new administrative practices or information systems that will significantly change or affect the collection, use and disclosure of personal information, McMan may complete a Privacy Impact Assessment (PIA) that describes how the new initiative will affect privacy, and what measures McMan will put in place to mitigate risks to privacy. See PRIV-1-9 Privacy and Information Security Assessments for additional details.
7. McMan employees and persons acting on behalf of McMan report all violations and breaches of information security as soon as possible to McMan's Privacy Officer. This enables the Privacy Officer

to take corrective action to resolve the immediate problem and minimize the risk of future occurrence.

8. The minimum retention period for records retention under FOIP is one (1) year. Beyond that, the retention periods are set according to the business requirements, contractual agreements and applicable by-laws and schedules of McMan. Personal information that was used to make a decision about an individual will be kept for at least one year after the decision has been made.

Physical Safeguards

9. All McMan records, both on-site and off-site, are held and stored in an organized, safe, and secure manner in accordance with information security standards.
10. Appropriate fire detection and extinguishing devices are located in areas where personal information is stored.
11. McMan's records are not accessible by unauthorized persons. In areas where unauthorized persons are present, measures will be taken to ensure that files are not left unattended or accessible.
12. Computers or monitors that are left unattended in reception areas or areas where personal information is processed are secured and logged off, either manually or by default timer.
13. All equipment storing electronic personal information is secured by locked cabinets or rooms within McMan when not under direct supervision by employees.
14. McMan records or equipment holding records (e.g., laptop computers, USB sticks, portable storage devices) may only be left locked in the trunk of an unattended vehicle when employees are transporting them.
15. An employee accompanies visitors to private or semi-private areas, including program employee areas, to ensure that only authorized individuals are present.
16. Appropriate measures are taken to control the distribution of keys/fobs or passcodes, and to ensure they are returned or changed after employment or association with McMan has ended.
17. Confidential information will be treated with sensitivity. Employees will take care when sharing confidential and personal information if conversations can be overheard or intercepted by unauthorized individuals.
18. Confidential, restricted, or sensitive information that is transmitted by mail or courier will be sealed, marked accordingly, and directed to the attention of the authorized recipient.
19. McMan employees will verify the identity and credentials of courier services used for the transportation of personal information.
20. Fax machines and printers that may be used to send or receive confidential information are located in a secure area, if possible. Whenever possible, employees will use preprogrammed numbers to send fax transmissions and will review the numbers every 6 months to ensure they are still accurate. All fax transmissions will be sent with a cover sheet that indicates the information being sent is confidential (see Security of Facsimile and Electronic Mail Transmissions, below). Reasonable steps are taken to confirm that confidential information transmitted via fax is sent to a recipient with a secure fax machine.
21. Information that is not confidential or sensitive in nature will be recycled. Confidential or sensitive information is destroyed by shredding. Destruction of records subject to McMan's retention and destruction schedule will be documented by listing the records and / or files to be destroyed, the date

of destruction, and an employee's signature to confirm that the destruction occurred. The destruction of transitory records does not need to be documented.

22. All information will be deleted using secure data wiping techniques prior to disposal of electronic data storage devices (e.g., surplus computers, internal and external hard drives, cell-phones diskettes, tapes, CD-ROMS, etc.), or the device(s) will be destroyed.

Technical Safeguards

23. Firewalls, intrusion detection software, or other technical means to protect internal McMan networks carrying identifiable personal information is in place to prevent unauthorized use and malicious software.

24. Access to data and application systems to personal information is limited by each McMan employee's functional role and need to know.

25. Employees of McMan access and use information systems under their assigned User ID. The use of another person's assigned User ID is prohibited. The assigned User ID restricts access to data and application systems to that information based on their functional roles and need to know.

26. Access to McMan information systems is controlled and password protected. Passwords are kept confidential at all times, and will not be posted publicly, or shared with other employees. If a computer is left unattended, it will be protected against unauthorized access by manual or automated logout requiring authentication to re-enter the system.

27. Personal electronic devices are not permitted to access McMan's network environment (ex. are limited to using McMan's public network for service participants and visitors).

28. All McMan electronic information shall be stored on McMan protected network drives which have proper access controls to ensure only authorized access. Storing McMan electronic information on memory devices (ex. USBs, memory cards, etc.) and electronic devices is not permitted unless specifically authorized and the information is encrypted according to McMan policies, procedures, and standards. McMan electronic information cannot be stored on personal devices.

29. Personal information is not permitted to be sent by e-mail or transmitted over the internet or external networks without the use of appropriate security safeguards, such as encryption and authentication. E-mail messages must also contain a confidentiality notification (see Security of Facsimile and Electronic Mail Transmissions below).

30. To detect unauthorized access and prevent modification or misuse of user data in applications, systems may be monitored to ensure conformity to access policies and standards. Appropriate security controls, such as event logs, will be implemented and reviewed as required.

31. Computer systems that hold critical or sensitive information will be backed up on a daily basis, at minimum. Backed up information is stored in a secure environment off-site. Information that is intended for long-term storage on electronic media (e.g., tape, DVD, disk, USB, portable hard drive) will be reviewed on an annual basis to ensure the data is retrievable, and to migrate the data to another storage medium if necessary.

PROCEDURE

Security of Facsimile and Electronic Mail Transmissions

32. All Transmissions

    a. Limit transmission to circumstances where it is immediately necessary for time-sensitive or functional reasons and to the least amount of information possible.

    b. All transmissions are accompanied by the following statement:

    This information is intended for the identified recipient only and may contain information that is privileged or confidential under law. If you are not the intended recipient, you are hereby notified that any dissemination or communication of this information is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the contact address or number indicated.

33. McMan users will only send or forward very large (10MB) documents or attachments when absolutely necessary. If you need to send or forward documents or attachments larger than 10MB, please contact IT Support.

34. Electronic Mail

    a. Do not transmit by e-mail over a service other than McMan e-mail service, with the exception of members of McMan South's Regional Board of Directors.

    b. Do not transmit identifiable personal information by e-mail to an external or public zone unless the information is secured by encryption.

    c. Verify access permissions and correct link before sharing SharePoint links.

    d. Do not include identifiers or personal information in the subject header of the mail.

    e. Remove all personal identifiers from the message if possible, including other email address.

    f. Verify all addresses as correct before sending messages.

    g. Develop, update and use e-mail addresses from address book.

    h. McMan users will not open e-mail message attachments from suspicious or doubtful sources. If in doubt, contact IT or the sender, through their confirmed email address, and verify the content of the message.

35. Facsimile Transmissions

    a. Where information is sent by fax transmission, the responsibility to confirm secure receipt of the information lies with the sender. Check the recipient's fax number prior to dialing. Ensure the recipient's machine is in a secure area. Ensure the recipient is available to receive the fax and confirm transmission of the information.

    b. An approved McMan Fax Transmission Cover Sheet must be completed and accompany the information transmitted.

    c. To ensure accuracy in dialing, confirm the number being dialed by visual check on the fax machine display. For frequently dialed numbers, use the automatic dialing feature to minimize incorrect dialing.

    d. Where possible, use available security features on the fax machine, i.e. confidential mailboxes to ensure the confidentiality of information, or encryption of the fax.

e. Verify that documents were received at the correct number.

f. If it is determined that the transmission was received by a wrong number:

- contact the recipient and ask them to return or destroy the documents,
- retain copies of all information sent, and
- report the incident as an information security breach to McMan's Privacy Officer.

36. Inspections of E-mail Messages

a. McMan may view, monitor or inspect any messages sent or received using McMan's system. Examples of when this may occur include, but are not limited to:

- investigate information security incidents;
- support an urgent, time-sensitive action;
- investigate compliance with McMan Policy or Procedures;
- maintain McMan information systems; and
- comply with a court order or statutory requirement.

b. Where access to e-mail is deemed necessary, McMan will attempt to inform the affected users prior to any inspection disclosure of e-mail records, except when such notification would be detrimental to an investigation of possible violation of the FOIP Act or McMan Policy or Procedures.

37. Filing and Retention of E-mail messages

a. E-mail messages are considered records and therefore subject to the standards for classification and retention in the Records Retention and Disposition (Privacy) Policy. Messages that must be retained as master records should be either:

- transferred from the e-mail directory to a secure and maintained electronic file directory such as SharePoint, or
- printed out and filed in the appropriate paper file.

APPENDICES

Appendix 4 - Confidentiality Agreement