POLICY STATEMENTS
Policy No. 5.1
Sensitive Information

Effective Date:
August 1, 2014

This policy supersedes Policy No. CORP 5 dated May 9, 2013. It expands the policy to cover all sensitive information, including electronic and written or printed sensitive information. It also updates the definition of Sensitive Information, expands the section on employee education, requires Enterprise Technology Services (ETS) to document possible losses of Sensitive Information and adds approved exceptions to the policy in certain emergency circumstances.

I. PURPOSE

A. This Policy establishes common definitions for different types of sensitive information used throughout the Corporation and sets forth policy for the identification and protection of sensitive information.

B. Legislation in place requires public disclosure in the event of real or suspected mishandling of personal information. Various state and federal laws require companies to report lost or stolen personal information, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes-Oxley Act of 2002 and the Payment Card Industry standards; these types of legislation necessitate plans to identify, assess and mitigate risks associated with the Corporation's handling of personally identifiable information as well as other sensitive information.

II. SCOPE

A. The provisions of this Policy apply to MDU Resources Group, Inc. and all divisions and subsidiaries directly or indirectly majority-owned by MDU Resources Group, Inc., collectively referred to as the "Corporation."

III. DEFINITIONS

A. The sensitivity of information defines the level of access controls and the degree of special precautions required to protect the information. The Corporation's information will be classified as "Sensitive Information", "Limited To Business Information" or "Public Information."

1. "Sensitive Information" includes both sensitive personal information and sensitive corporate information.

   Unauthorized access to sensitive personal information, or personally identifiable information (PII), may result in a significant invasion of privacy or may expose individuals to significant financial risk. The following are generally considered PII:

   a) Social security number
   b) Personal identification information, such as a driver's license number or any other department of transportation issued identification number or a passport number
   c) Customer account number, password or pin
   d) Any personally identifiable customer information
   e) Credit card, debit card or bank account information
   f) Medical or health care information

Depending on state law, other information may be considered PII when accompanied with first initial and last name, such as date of birth or an identification number issued by an employer (employee ID). If you have questions about whether certain data constitutes PII, contact the Legal Department.

Unauthorized access to or modification of sensitive corporate information may result in direct, materially negative impacts on the finances, operations or reputation of the Corporation. The following are generally considered sensitive corporate information:

a) Financial reporting, financial planning and forecasting data prior to public release
b) Business plans, sales and marketing plans, merger, acquisition and divestiture plans
c) Employee records, including home address and home phone numbers
d) Incentive plan participant information
e) Legally privileged or protected information

2. "Limited To Business Information" includes information that is intended for use by the Corporation's personnel only and requires appropriate controls applied to limit the chance of inadvertent exposure to non-Corporation personnel. The exposure of this information would not break any legal, regulatory or specific business confidentiality requirements and would not materially adversely affect the Corporation or the public. Examples include but are not limited to:

a) Department phone directories that do not include personal information
b) Human resources information such as salary ranges, policies and benefits

3. "Public Information" includes Information that receives widespread disclosure and does not require special precautions or controls to limit access to the information. There are no requirements for the handling of Public Information in this Policy. Examples include but are not limited to:

a) Annual reports
b) Issued press releases and public announcements
c) Job postings

B. "Data Protection" means applying technical and administrative controls to reduce or mitigate the risk of unauthorized access or unlawful processing of Sensitive Information and against the accidental loss or destruction of Sensitive Information.

C. "Data Owner" is the individual who has ultimate responsibility for Data Protection and would be held responsible when it comes to protecting the Corporation's information. The Data Owner is responsible for identifying Sensitive Information and determining how the Sensitive Information should be protected in accordance with this Policy.

D. "Data Custodian" is the individual or group who is responsible for the maintenance and protection of the information.

1. The Data Custodian of non-electronic information is usually the Data Owner.

2. The Data Custodian of electronic information may be the Data Owner and/or the information technology department. For electronic information, the Data Custodian's duties may include information backups, implementing security controls directed by the Data Owner, restoring information from backups and fulfilling requirements set out in information technology policies.

E. "Users" mean individuals that use, process, store or transport Sensitive Information as part of their job duties. Users are responsible for ensuring the Sensitive Information they use is not mishandled.

F. "Encrypted" and "Encryption" mean the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge (usually referred to as a key) resulting in encrypted information. Encryption also implicitly refers to the reverse process or decryption to make the encrypted information readable again (i.e. to make it unencrypted).

G. "ETS Help Desk" means the Corporation's enterprise technology services help desk available at 1-800-431-5728 or 1-701-530-1212.

H. "IT Leaders" means the Corporation's Information Technology Leaders group.

I. "Managers" means employees of the Corporation who are executives, directors, managers or supervisors and employees who have management responsibility for other employees of the Corporation.

IV. IDENTIFICATION AND EVALUATION OF SENSITIVE INFORMATION

A. The Corporation's Managers will be responsible for identifying how Sensitive Information is being used in their organizations and identifying the Data Owners of this information. Data Owners will be responsible for knowing what Sensitive Information they own and where that Sensitive Information is stored.

B. The Corporation's Managers, in conjunction with the Data Owners, Data Custodians and the Legal Department, will evaluate the legal and competitive risks associated with the Sensitive Information and direct that adequate controls for the protection of this information be established.

V. PROTECTION OF SENSITIVE INFORMATION

A. Data Owners are responsible for ensuring the established controls for the protection of Sensitive Information are being followed. Users should handle Sensitive Information in accordance with the established controls.

B. Administrative – Education and Lost Information

1. All Users and Data Custodians of Sensitive Information should be provided educational information regarding the handling of Sensitive Information by their Manager and the Corporation. The Appendix to this policy, "Frequently Asked Questions – Sensitive Information Policy, may be used to help educate employees about this policy.

2. All Users who suspect they may have lost a) written or printed Sensitive Information, b) electronic Sensitive Information, or c) a device possibly containing electronic Sensitive Information, or are otherwise aware of any other suspected loss or breach of Sensitive Information must immediately report the incident to the ETS Help Desk or an IT Leader, who will notify the Corporation's Legal Department.

C. Access to Sensitive Information and Limited to Business Information

1. Sensitive Information
   a) Access to Sensitive Information will be limited to Users on a "need-to-know" basis. Data Owners will ensure access to Sensitive Information is provided only to those individuals who need to know this information.
   b) Requests for access to electronic Sensitive Information will follow standard computer authorization requests (i.e. security request procedure).

2. Limited to Business Information
   a) Access to Limited to Business information will be limited to employees only.
   b) Requests for access to electronic Limited To Business information will follow standard computer authorization requests (i.e. security request procedure).

D. Handling Physical Sensitive Information

1. Sensitive Information will be stored in an area or container that can be locked to prevent unauthorized access or theft when the information is not being actively used. Sensitive Information will be controlled to prevent unauthorized access or theft when it is being moved between locations.

2. Sensitive Information will not be stored at a third party's location unless approved by the Data Owner. Sensitive Information that is approved for storage at a third party's location must be protected by defined controls.

3. Sensitive Information will be destroyed in a manner that prevents re-creation of the information. Shredding is one method for destruction of physical material containing Sensitive Information.

E. Handling Electronic Sensitive Information

1. Sensitive Information will not be stored on laptop computers, removable media such as USB drives, smart phones, tablets, or other smart devices unless the devices are encrypted and password protected in a manner that is approved by the IT Leaders. If a User is unsure if he/she is storing Sensitive Information, he/she should contact the ETS Help Desk. If a User is unsure if his/her device is encrypted and/or password protected, he/she should contact the ETS Help Desk.

2. Sensitive Information will not be saved or stored on an employee-owned computer or electronic device.

3. Sensitive Information will not be delivered to third-party contractors unless there is a nondisclosure agreement between the Corporation and the contractor wherein the contractor agrees to handle the Sensitive Information in a manner consistent with the provisions in this Policy or applicable privacy law, whichever is more restrictive.

4. Sensitive Information will not be stored on a third party's computer or electronic device or on a third party cloud provider's server, computer or electronic device without the knowledge and approval of the Data Owner of the Sensitive Information, the corporation's ETS department director, the General Counsel in the Legal Department and without the nondisclosure agreement described above in paragraph 3.

5. Sensitive Information will not be transported electronically outside of the Corporation's computer network through email or any other electronic file-transfer method without Encryption and the knowledge and approval of the Data Owner of the Sensitive Information.

6. All laptops, removable media intended to store Sensitive Information, smart phones, tablets, and other smart devices purchased by the Corporation after the original Effective Date of this Policy (May 9, 2013) will have encryption software installed and activated. Such software will have the ability to be centrally monitored for compliance with this policy.

7. All server backup media purchased by the Corporation after the original Effective Date of this Policy (May 9, 2013) that contains Sensitive Information will be encrypted.

8. All computing equipment, electronic media or other electronic devices that have the capability to store Sensitive Information will use a wiping program or other acceptable means to erase all of the Corporation's data on the device prior to reassigning or redeploying the device to a new user within the Corporation and prior to discarding the device, or the electronic media will be destroyed prior to discarding the device.

E. Additional Information Regarding Electronic Sensitive Information

1. Data-base logging will be considered for databases containing Sensitive Information in order to monitor or report possible compromise attempts of this information.

2. Based on the risks associated with the loss of specific Sensitive Information, additional controls may be necessary, such as the Encryption of this information at the source server location.

VI. BREACH OF DATA/INCIDENT HANDLING

A. All data breaches must be reported immediately to the ETS Help Desk or an IT Leader, who will notify the Corporation's Legal Department and the ETS security group.

B. ETS will document losses of Sensitive Information in an electronic system.

VII. VIOLATIONS OF THIS POLICY

A. Any employee who violates this policy may be subject to disciplinary action, up to and including termination of employment.

VIII. EXCEPTIONS

A. Exceptions to this Policy must be brought to the Corporation's IT Leaders. After review, the IT Leaders will make a recommendation to the Chief Financial Officer of MDU Resources Group, Inc., who must approve exceptions to this Policy.

B. ETS will maintain documentation of exceptions to this Policy.

C. Approved Exceptions

1. If the Corporation's email system is not available in an emergency situation, confidential employee contact information may be sent to and from employees' alternative email accounts when approved by a business unit president.

2. If the Corporation's email system is not available in an emergency situation, Sensitive Information may be sent to and from a secure third-party service provided by the Corporation.

IX. ADMINISTRATION

A. The Chief Financial Officer of MDU Resources Group, Inc. has the responsibility for the overall administration of this Policy.

B. Establishment and implementation of procedures to administer this Policy are the responsibility of the Chief Financial Officer of MDU Resources Group, Inc.

Reviewed by: /s/ Doran N. Schwartz
Doran N. Schwartz
Vice President and Chief Financial Officer

Approved By: /s David L. Goodin
David L. Goodin
President and Chief Executive Officer

Appendix

Sensitive Information Policy Frequently Asked Questions

- Why do we have this policy?
  - It defines sensitive information and how employees must protect it.
- Who is affected by this policy?
  - This policy applies to anyone within MDU Resources and its subsidiary companies who handles or receives sensitive information in any form, including electronic files and printed or written materials.
- What is sensitive information?
  - Sensitive personal information includes:
    - Social security number(s).
    - Driver's license number(s) or other Department of Transportation-issued identification number(s) or passport number(s).
    - Information that identifies customers, such as personal information, account number(s), password(s) or PIN(s).
    - Credit card, debit card or bank account information.
    - Medical or health-related information.
  - Sensitive corporate information includes:
    - Financial reporting, financial planning and forecasting data prior to public release.
    - Business plans, sales and marketing plans, merger, acquisition and divestiture plans.
    - Employee records, including home addresses and phone numbers.
    - Incentive plan participant information.
    - Legally privileged or protected information.
- Who is responsible for identifying how sensitive information is handled?
  - The corporation's Managers are responsible for identifying how sensitive information is handled.
- Who is responsible for knowing what sensitive information is held, where it is stored and ensuring that it is protected?
  - People who own the sensitive information, as identified by the corporation's Managers, are responsible for that information, including keeping track of where it is stored and keeping it safe.
- How should physical sensitive information be handled?
  - Physical sensitive information, such as items in printed or written form, must be kept in a secure area such as locked storage. Sensitive information will not be stored at a third-party location unless approved by the information's owner. Sensitive information must be destroyed in a way that prevents anyone from re-creating the data, such as by shredding.

- How should electronic sensitive information be handled?
    - Devices such as laptops, USB flash drives, smart phones, tablets, etc. that store electronic sensitive information must have company-approved encryption and password protection. Employees cannot store sensitive information on personally owned computers or other electronic devices. Sensitive information that is electronically transmitted must be sent through encrypted email or electronic file transfer.
- How should data breaches be reported?
    - Employees should immediately report violations of the sensitive information policy to the ETS Help Desk or an IT leader.

Protect Our Sensitive Data

- You are responsible for protecting sensitive information.
- Always store sensitive information in a secure location.
- Ensure all of your electronic devices are password protected.
- Ensure your electronic devices are encrypted.
- Properly dispose of sensitive information, either by shredding documents or fully deleting files.
- If you have questions or concerns about sensitive information, contact the ETS Help Desk at 1-800-431-5728 or (701) 530-1212.