Computer Account Request form for County Feedlot Program

Doc Type: User IDS/Profiles/Authorizations/Passwords

Instructions:

County Feedlot Officers and additional primary users (one form per person) complete the "Authorized Associate" portions of this request form. Scan and email signed form to Michelle Oie at Michelle.oie@state.mn.us.

I, Randall G. Hukriede, Manager, Feedlot Section, MPCA Watershed Division, would like to request that a computer account be activated for:

Print name: _____ County name: _____

(hereinafter to be identified as Authorized Associate)

Email address: _____ Telephone number: _____

Mailing address: _____ City, State and Zip: _____

MN.IT Services Accommodations Needed

Access to: ☒ Unless specifically requested access will be equivalent to a new MPCA employee.

Applications: ☐ Other (specify): _____

Remote access needed: ☒Citrix Account/MPCA RSA Token **(See reverse side)**

Activation date: November 15, 2010 Termination date: TBD by Feedlot Program Staff

(All Authorized Accounts expire one year from activation date, unless otherwise specified.)

All Parties Must Read Before Signing

- I understand that MN.IT Services only creates the computer accounts, and that, in order to gain access to particular Information Systems (TEMPO, TALES, email) for this Authorized Associate, it may be necessary for me to contact the department Database Champion) to which authority has been given over said Information System.
- I further understand that, after a new account has been assigned to the Authorized Associate account name and the initial password will be distributed.
- County staff is responsible to ensure that MN.IT Services is notified when the user for whom this account is created leaves their company/agency or no longer requires access to the MPCA network.

Computer Account Use Requirements

(a) Computer accounts are created for individual users. Each user must use only those computer accounts that have been created for his/her use. The negligence of an account owner in revealing an account name and password is not considered authorization for use.

(b) Account owners are responsible for all use of their accounts. Account owners must make appropriate use of the system protection features (such as regularly changing passwords and maintaining confidentiality of passwords) and must take precautions against others obtaining access to their computer resources.

(c) MPCA Information Systems and System Resources are intended only for use in conducting MPCA business. Usage not related to MPCA business is strictly prohibited. Use of assigned accounts is limited to the assigned user and to those computer processes, data, systems, and resources expressly made available through the account.

(d) Account owners are responsible for compliance with all Agency/State computer use policies and procedures. (See attached policies.)

(e) Data practices. Any not public data shall be handled in a confidential manner, will not be distributed or copied from state systems without appropriate signed authorization. MPCA is required to be notified of any known data breach of its systems and in accordance to State Statute 13.055.

As an Authorized Associate owner, I agree to abide by the above requirements, which I have read and fully understand. By my signature below, I also acknowledge that I have read this form and understand the process by which I will receive my account.

Authorized Associate (required)

Print name: _____

Signature: _____

Date: _____

MPCA Section Manager (required)

Print name: Randall G. Hukriede

Signature: _____

Date: _____

Authorized Associate (i.e., County staff Supervisor) responsible for notifying the MPCA of any changes to the account (i.e., termination date):

Print name: _____ Phone: _____

Token Acquisition

For computer connectivity from outside of the agency.

Important: Users must attend MPCA training prior to the distribution of the assigned token.

Type of Token Requested (only select one):

- ☐ IOS System (Apple Product) on your mobile device*
- ☐ Android System Soft Token on your mobile device*
- ☐ On-Demand Link – Hyperlink on your computer

*****The token is programmed to expire on a scheduled date listed in the app information icon. It is recommended you contact the service desk at least 30 days in advance to coordinate the delivery of a replacement token.

Authorized Associate (required)

Print name:_____

Signature:_____

Date:_____

MPCA Section Manager (required)

Print name: Randall G. Hukriede

Signature:_____

Date:_____

Token Usage Guidelines

Business use restrictions. Equipment and software furnished by state agencies remains the property of the state and are subject to the same business use restrictions as in-office property. Employee-owned software shall not be installed on state-owned equipment.

Notice to MN.IT Services and Supervisor. For security purposes users are responsible for promptly notifying MN.IT Services (Help Desk 651-297-1111) and their supervisor of lost or stolen equipment (i.e., token). Also, notify MN.IT Services of any equipment malfunction or failure of either state-owned or employee-owned equipment. If the malfunction prevents the user from performing assigned tasks, the user must notify the user's supervisor immediately.

Return of equipment. The equipment must be returned in good physical condition, and proper operating condition, other than instances when the equipment experiences normal malfunction.

Personal use prohibited. Equipment, software, data, supplies, and furniture provided by the State for use at the user's home work location are for the purposes of conducting state business and may not be used for personal purposes by the employee or non-employees of the state.

Policy compliance. Users are responsible for reading, understanding, and following all applicable agency and state policies related to the use of state-owned electronic equipment and technology. Violations of policy may subject the user to disciplinary action up to and including discharge.

Violation of the above practices may result in refusal of service and disciplinary action.

Data Privacy Acknowledgement form for County Feedlot Program

Doc Type: User IDS/Profiles/Authorizations/Passwords

Minn. Stat. § 13.01, subd. 1 *states, "All government entities shall be governed by this chapter."*

Minn. Stat. § 13.01, subd. 2 *states, "This chapter may be cited as the 'Minnesota Government Data Practices Act."*

Minn. Stat. § 13.03, subd. 4(c) *states, "To the extent that government data is disseminated to a government entity by another government entity, the data disseminated shall have the same classification in the hands of the entity receiving it as it had in the hands of the entity providing it."*

Minn. Stat. § 13.08, subd. 1 *states a "government entity which violates any provisions of this chapter is liable to a person…who suffers any damage as a result of the violation."*

Minn. Stat. § 13.09 *states, "Any person who willfully violates the provisions of this chapter or any rules adopted under this chapter is guilty of a misdemeanor. Willful violation of this chapter by any public employee constitutes just cause for suspension without pay or dismissal of the public employee."*

Acknowledgment

As an employee of a county governmental office and in partnering with the Minnesota Pollution Control Agency (MPCA), I understand that I am bound by the laws concerning data as described in Chapter 13 of Minnesota statutes, known as the Minnesota Government Data Practices Act (MGDPA).*

To the extent necessary to fully execute work for the MPCA, the undersigned may have access to data that are classified as not public. Any not public data collected, created, stored, maintained, disseminated, used or overheard in the course of the performance of this work may be disclosed or disseminated only to those county employees whose work assignments reasonably require access in fulfilling the county employee's obligations to the MPCA and these data must be managed according to their proper classification. I understand that I am responsible for protecting the logon and password privileges I am requesting.

I understand that my employer and/or I could suffer penalties for violating the MGDPA (or any rules adopted under this chapter).

* Minnesota Government Data Practices Act, Minn. Stat. ch. 13 https://www.revisor.mn.gov/pubs/.

Print name: _____ Email: _____

Signature: _____ Date: _____

MINNESOTA POLLUTION CONTROL AGENCY

Administrative Policy

Administrative Policy No. i-admin8-07

Policy title: Security information

Policy type: General

Policy owner: Information Systems Management Team

Effective date: September 2020

Replaces or Supersedes: Security information dated January 15, 2014; May 31, 2018; and Security data dated April 2005

Date of Policy review: Fall 2020

Policy statement: The Minnesota Pollution Control Agency (MPCA) has a statutory responsibility to protect the data in its possession that are classified as security information.

Peter Tester Digitally signed by Peter Tester Date: 2020.11.13 08:19:53 -06'00'

Peter Tester, Deputy Commissioner

Purpose: This policy provides MPCA staff members, county feedlot officers, contractors, and volunteers with the necessary information on managing not public data classified as security information, and on the proper management and protection of this data type within the Agency.

Scope: This policy applies to all MPCA staff members, county feedlot officers, contractors, and volunteers. All Agency staff members, county feedlot officers, contractors, and volunteers are expected to understand and comply with the requirement to properly manage and protect security information. The policy applies to all information in the possession of the Agency in any of its offices in electronic or paper form.

Background: Under the Minnesota Government Data Practices Act, Minn. Stat. ch. 13, data are classified as public unless a federal law, state statute, or temporary classification creates a not public classification for the data. One statutory category of not public data is termed “security information.”

Pursuant to Minn. Stat. § 13.37, subd. 1(a), security information means “government data the disclosure of which the responsible authority determines would be likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury.” The responsible authority is the individual who

oversees the collection, dissemination, and use of data within a governmental entity. At the MPCA, the responsible authority is the General Counsel.

Governmental entities have discretion in determining the data in their possession that may be classified as security information. The MPCA periodically reviews the types of data that it maintains to determine if they fit the definition of security information. The review results are found in the Agency security information table below.

The table may not include all data types that should be classified as security information. If staff feel that a data type should be added to the table or are uncertain about the classification of certain data, they should contact the MPCA's Data Practices Coordinator or General Counsel.

Procedure for the management of requests for data classified as security information

Since the data types listed in the table are classified as not public security information, the Agency must properly manage and protect such data. This means not placing them in public files or reports, labeling them as not public, storing them securely, not sharing the data with others who have no business reason to access them, not providing them to requesters, and similar methods.

Pursuant to Minn. Stat. § 13.03, subd. 3(f), if MPCA receives a request to have access to or to obtain copies of any of its security information, it must inform the requester that the data cannot be provided, either orally at the time of the request or in writing as soon as possible. Additionally, the Agency must inform the requester that Minn. Stat. § 13.37, subd. 1a and subd. 2 are the state statutory provisions upon which the classification is based.

Review of agency files

Many of the data types listed as security information in Table 1 may be contained in reports or monitoring documents in a site's paper or electronic files. Staff members are responsible for reviewing their files, electronic or paper form, for the presence of not public security information. Supervisors and managers should work with their staff to ensure that files are reviewed for not public data security information prior to being made available to the public in response to a file review/information request, before they are put into any of the agency's data management systems, the Agency's electronic document management system, or before being sent to archival storage. All staff members must cooperate with file managers to review files for not public security information in a timely manner when asked.

For more specific information regarding how to manage not public data located in Agency files, electronic or paper form, see the data practices page on the agency's internal website, The Lorax.

All new data received by MPCA staff that constitute security information should be identified, segregated from the public files and reports, and secured upon receipt of the data.

Agency agreements with other governmental entities

Pursuant to Minn. Stat. § 13.03, subd. 4(c), when a governmental entity (i.e., a state agency, a statewide system, or a political subdivision) disseminates data to another governmental entity, the data in question must retain the same classification at the entity receiving the data that they have at the entity that provided them. Therefore, Agency staff who receive data from another governmental entity that is classified as not public by that entity must properly manage the data.

*One example is the Minnesota Department of Health's (MDH) policy on access, distribution, and use of secured drinking water related data as it pertains to locational data of wells for public water systems. MDH classifies that data as non-public security information and when that data is provided to the MPCA

by MDH, it must also be treated by MPCA staff as we would our own security information even if we do not agree with MDH's classification.

Agency security information

Data type	Data description
Chemical plants and refineries	Specific blueprints showing details of tanks, valves, pump stations or piping within a site. Geospatial data derived directly from blueprints are included. Geospatial data derived from air imaging are not included.
Continuity of operations plan	Information documenting threats and vulnerabilities facing the agency, the risks that are being mitigated and the unmitigated risks that remain. Information regarding key positions, functions and/or contacts required for response and/or recovery from an incident focused on the agency. Information regarding the addresses of recovery locations and/or redundant sites of key systems. Information regarding the cause of an incident involving the agency and the agency's response. Information regarding the critical supply chain. Procedures and processes detailing response and recovery from an incident.
Drinking water treatment plants and *Municipal well locations (see section regarding agreements with other agencies)	Specific blueprints or details of chemical storage, disinfection systems, and intake structure designs. Geographic information system shapefiles for municipal well data from MDH.
Hazardous waste treatment storage or disposal facilities	Specific blueprints showing details of piping, pump stations, tanks, or valves within a site for facilities containing 1,000,000 gallons or more of hazardous waste.
Incident operational security	Documents or plans such as incident action plans, security response plans, situation reports, etc. that contain security information pertaining to a specific event in which release of the information could jeopardize efforts to protect the public. Please note, this information is classified as not public data only temporarily during the time period surrounding the event.
Large aboveground and underground storage tank facilities	Specific blueprints showing details of piping, pump stations, tanks, or valves within a site for facilities containing 1,000,000 gallons or more of oil or hazardous substance in tank storage at any time.
Municipal stormwater	Municipal stormwater outfall locations above surface water intakes and drinking water intakes.
Personal financial data	Data that a prudent person would not make publicly available so as to avoid jeopardizing the security of his/her information, possessions or property against financial/identity theft, tampering or improper use, such as charge card numbers, checking account and other banking numbers, credit card numbers, debit card numbers, insurance policy numbers, securities numbers, and other similar account/card numbers.
Pipeline systems and railroad systems	Blueprints showing details of pipelines, pump stations, valves etc. Geographic information system shapefiles for pipeline routes and railroad "high consequence areas" (HCAs). Portions of emergency response plan (refer to unit for more detailed information). Portions of railroad emergency response plans (refer to unit for more detailed information).

Data type	Data description
Power plant intakes and outfalls	Specific blueprints or details of cooling water intake and discharge structures such as emergency locations within the plant property, locations of emergency intakes, pumping stations on site, etc.
Special air monitoring facilities	Location and operation details of air monitors that may be installed in Minnesota for biological contaminant detection.

Definitions

Shapefile: Geospatial vector data format for geographic information system (GIS) software.

High Consequence Area (HCA): May include high population areas, unusually sensitive areas, and commercially navigable waterways.

Responsibilities

All MPCA staff members, county feedlot officers, contractors, and volunteers are expected to be aware of and comply with this policy. Failure to comply with this policy may subject a staff member, county feedlot officer, contractor, or volunteer to disciplinary action and penalties as provided in Minn. Stat. ch. 13. Penalties may include suspension, dismissal, or referring the matter to the appropriate authority who may pursue criminal misdemeanor charges.

MINNESOTA POLLUTION CONTROL AGENCY

Administrative Policy

Administrative Policy No. i-admin8-12

Policy title: Records and data management

Policy type: General

Policy owner: Information Systems Management Team

Effective date: September 2020

Replaces or Supersedes: October 15, 2014; August 30, 2016

Date of Policy review: Fall 2020

Policy statement: State law requires governmental entities to "make and preserve all records necessary to a full and accurate knowledge of their official activities" (Minn. Stat. § 15.17, subd. 1). Documents that are not necessary to retain for these reasons are to be destroyed in accordance with the Agency's records management program. However, no record or data that are subject to a legal hold may be destroyed for any reason until the hold has been released.

Peter Tester Digitally signed by Peter Tester Date: 2020.11.13 08:25:41 -06'00'

Peter Tester, Deputy Commissioner

Purpose: The *Records and data management* policy establishes requirements for managing Minnesota Pollution Control Agency (MPCA) data and information defined as "government data" and /or "government records" in accordance with applicable laws, regulations, policies and established practices. The policy will ensure public access to governmental data that are classified as public, the protection and security of not public data and proper management of MPCA governmental records.

This policy:

1. Ensures the proper management and retention of governmental data and records created by or under the control of the MPCA, whether in paper or electronic form;
2. Recognizes proper data management as an agency-wide responsibility;
3. Establishes and maintains an active, continuing program for the economical and efficient management of MPCA governmental records (Minn. Stat. § 138.17, subd. 7); and
4. Delineates specific minimal responsibilities and roles of MPCA employees, contractors, and volunteers in the proper management of data and records.

To satisfy state law, the MPCA's records management program is described in a document identified as the *Records and data management manual* (Manual) that is modified as necessary to maintain the program consistent with changes in legal requirements. The Manual includes instructions and guidance on the implementation of this policy, an inventory of the type of records in the MPCA's custody and a *Records retention schedule* approved by the State Records Disposition Panel, which establishes a time period for the retention or disposal of these records (Minn. Stat. § 138.17, subd. 7). Data that are not a record or otherwise required to be preserved should be discarded after they have fulfilled their purpose to avoid the unnecessary expense and effort required to preserve them.

Scope: This Policy applies to all MPCA employees, county feedlot officers, contractors, and volunteers.

Definitions

Government data: All data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or conditions of use" (Minn. Stat. § 13.02, subd. 7). All governmental data are presumed to be public and accessible by the public for both inspection and copying unless there is federal law, a state statute or a temporary classification of data that provides that certain data are not public (Minn. Stat. § 13.01, subd. 3 and Minn. Stat. § 13.03, subd. 1).

Government records: "State and local records, including all cards, correspondence, discs, maps, memoranda, microfilms, papers, photographs, recordings, reports, tapes, writings, optical disks, and other data, information, or documentary material, regardless of physical form or characteristics, storage media or conditions of use, made or received by an officer or agency of the state and an officer or agency of a county, city, town, school district, municipal subdivision or corporation or other public authority or political entity within the state pursuant to state law or in connection with the transaction of public business by an officer or agency." However, governmental records do not included data or information that do not become part of official transaction. (Pursuant to Minn. Stat. § 138.17, subd. 1 (b)(1))

State record: "A record of a department, office, officer, commission, commissioner, board or any other agency, however styled or designated, of the executive branch of state government; a record of the state legislature; a record of any court, whether of statewide or local jurisdiction; and any other record designated or treated as a state record under state law." (Pursuant to Minn. Stat. § 138.17, subd. 1 (b)(2))

Responsibilities

All agency employees, county feedlot officers, contractors, and volunteers shall:

1. Acknowledge reading this policy annually;
2. Attend required training provided or made available by the MPCA including, at a minimum:
    - Data practices;
    - The use of agency electronic document management systems (e.g., OnBase);
    - Identification of records and non-record material;
    - Records management responsibilities;
3. Manage all MPCA governmental records, whether on paper or in electronic form, in accordance with the Minnesota Government Data Practices Act, the Manual, program-level recordkeeping procedures and all applicable laws, regulations and policies;
4. Manage all governmental data, whether on paper or in electronic form, in accordance with the Minnesota Government Data Practices Act, the Manual, program-level recordkeeping procedures and all applicable laws, regulations and policies;
5. Only generate and use temporary copies of MPCA data or records when necessary and immediately destroy temporary copies after use;

6. Acknowledge that all data collected, created, received, maintained or disseminated in connection with work performed for or on behalf of the MPCA and/or with MPCA of State equipment, property or resources are governmental data;
7. Maintain purely personal papers and data separately from MPCA governmental data and records;
8. Be aware that all data, including data the employee may believe to be purely personal or privately owned (whether in paper or electronic form), may be determined to be governmental data if they were created with, stored on or accessed with MPCA or State equipment, property or resources, may have to be produced in response to a data practices request and may be subject to review, reproduction and distribution by the MPCA; and
9. Remove agency data and/or records from the MPCA offices only as authorized in the Manual.

All agency managers shall:

1. In consultation with the Records Manager, develop and document program-level recordkeeping procedures that define program-level work practices, roles and responsibilities, document filing/naming processes and keyword requirements for inclusion in the Manual;
2. Annually review program-level recordkeeping procedures and update them as necessary; and

The Document Services Unit, Information and Records Unit and /or Information Systems Management Team shall, in consultation with the Legal Service Unit:

1. Document the MPCA's records management program in the Manual and update or modify the Manual as necessary to reflect changing legal requirements, business needs, and evolving practices;
2. Work with program managers to help create program-level recordkeeping procedures;
3. Develop and provide training to employees on:
    - Data practices;
    - The use of agency electronic document management systems (e.g., OnBase); and
    - Records management responsibilities.
4. Maintain MPCA records in formats/media that will ensure a life expectancy specified in the Records Retention Schedule and maintain the equipment necessary to access these records in a readable format;
5. Destroy hardcopy documents after the images are properly digitized into electronic document management systems (e.g., OnBase) only when expressly permitted by general or program-specific requirements established in the Manual and all records according to the Records Retention Schedule; and
6. Audit compliance with this policy, conduct and/or coordinate annual compliance audits and testing of retention, legal hold and destruction procedures.

Accountability

Conduct that does not comply with this policy is not authorized by the MPCA and may subject an employee, county feedlot officers, contractor or volunteer to disciplinary action up to, and including termination. The appropriate action will be determined on a case-by-case basis, depending on the facts and circumstances.

MINNESOTA POLLUTION CONTROL AGENCY

Administrative Policy

Administrative Policy No. i-admin8-14

Policy title: Not public data protection

Policy type: General

Policy owner: Information Systems Management Team

Effective date: September 2020

Replaces or Supersedes: August 1, 2014; August 30, 2016

Date of Policy review: Fall 2020

Policy statement: All Minnesota Pollution Control Agency (MPCA) employees, county feedlot officers, contractors, and volunteers are expected to be aware of and comply with the requirement to properly manage and protect not public data at the MPCA.

Peter Tester Digitally signed by Peter Tester Date: 2020.11.13 08:27:45 -06'00'

Peter Tester, Deputy Commissioner

Purpose: This policy provides minimum requirements for managing not public data maintained at the MPCA in paper or electronic means, and the standards to ensure compliance with applicable laws and regulations regarding the protection of not public data, particularly data on individuals.

Scope: This policy applies to the not public data in the possession of the MPCA regardless of form, location or medium. “Not Public Data” comprise all data types that are classified as not accessible to the public or to personnel within governmental entities, except those personnel whose work assignments reasonable require access to the data. These include, but are not limited to, the following classifications of data as defined in the Minnesota Government Data Practices Act, found in Minn. Stat. ch. 13: Confidential and Private Data on Decedents, Confidential and Private Data on Individuals, Nonpublic and Protected Nonpublic Data Not on Individuals and any other data deemed not accessible to the public by court order, federal law, state statute or temporary classification.

Responsibilities

All agency employees, county feedlot officers, contractors, and volunteers shall:

1. Acknowledge reading this policy annually;
2. Attend required training provided or made available by the MPCA including Data Practices training;
3. Be knowledgeable about types of not public data maintained by the MPCA and within their programs;
4. Follow appropriate safeguards for all records containing not public data;
5. Follow procedures and guidance to access not public data only as required by work assignments;
6. Ensure, to the extent possible, that not public data will only be accessible to those whose work assignments require access to the data;
7. Share Agency not public data only when authorized by law;
8. Dispose of not public data in a manner that prevents the contents from being determined: and
9. Provide Tennessen warnings when necessary and use the not public data obtained via these warnings only for the purposes described in the warning if the not public data are needed for a different purpose, informed consent must be obtained.

All agency supervisors and managers, in addition to the responsibilities listed above for all employees, shall:

1. In consultation with the Information and Records Management Unit and the Document Services Unit, identify not public data collected and generated within their program areas;
2. Establish appropriate safeguards for all records containing not public data; and
3. Limit the MPCA's collection of not public data to that necessary for the administration and management of its programs.

In addition to responsibilities listed above, the Information and Records Management Unit and Document Services Unit, in consultation with the Legal Services Unit and Internal Controls, shall:

1. Create an inventory of not public data;
2. Conduct an annual security assessment of processes intended to safeguard any not public data on individuals maintained by the agency;
3. Conduct investigations in the event of a data security breach and provide the necessary notifications and reporting as required by law; and
4. Train employees, county feedlot officers, contractors and volunteers on the identification and proper management of not public data

Conduct that does not comply with this policy is not authorized by the MPCA and may subject an Agency employee, county feedlot officers, contractor or volunteer to disciplinary action and penalties as provided in Minnesota Statutes. Penalties may include suspension, dismissal or referring the matter to the appropriate authority, who may pursue criminal misdemeanor charges.