Information Security Roles and Responsibilities

Published: https://help.mncm.org

Original Date: 9/1/2019

Expected Review Date: 10/1/2020 Revised: NA

Disposition Instructions: Retain all previous versions of this policy for a minimum of 6 years from the date of creation or revision, whichever is later.

POLICY STATEMENT:

MN Community Measurement (MNCM) will support and maintain a viable information security incident management program. This policy reflects the data security roles and responsibilities for both MNCM and Collaborator.

SECURITY AND PRIVACY OFFICERS

The Security and Privacy Officers oversee the development and implementation of the MNCM Security Program. Specific responsibilities include:

- Ensure related compliance requirements are addressed, e.g., privacy, security, and administrative regulations associated with federal and state laws.
- Ensure appropriate risk mitigation and control processes for security incidents as required.
- Document and disseminate information security policies, procedures, and guidelines
- Coordinate the development and implementation of MNCM information security training and awareness program

MNCM DATA OWNER

A Data Owner is an MNCM staff member who has been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within MNCM.

The role of the Data Owner is to provide direct authority and control over the management and use of specific information. These individuals might be department heads, managers, supervisors, or designated staff.

Responsibilities of a Data Owner include the following:

Ensure compliance with MNCM polices and all regulatory requirements
Data Owners need to understand whether any MNCM policies govern their information assets.

Data Owners are responsible for understanding legal and contractual obligations surrounding information assets within their functional areas

Assign an appropriate classification to information assets
All information assets are to be classified based upon its level of sensitivity, value, and criticality to MNCM. MNCM has adopted four primary classifications: Public, Internal, Confidential, and Protected Health Information.

Understand how information assets are stored, processed, and transmitted
Understanding and documenting how information assets are being stored, processed, and transmitted is the first step toward safeguarding data. Without this knowledge, it is difficult to implement or validate safeguards in an effective manner.

Understand and report security risks and how they impact the confidentiality, integrity, and availability of information assets
Data Owners need to have a thorough understanding of security risks impacting their information assets. For example, storing or transmitting sensitive data in an unencrypted form is a security risk. Protecting access to data using a weak password and/or not patching vulnerability's in a system or application are both examples of security risks. Security risks need to be documented and reviewed with the appropriate Data Owner so that he or she can determine whether greater resources need to be devoted to mitigating these risks. Information Technology Services can assist Data Owners with gaining a better understanding of their security risks.

COLLABORATOR

All Collaborators have a critical role in the effort to protect and maintain MNCM information systems and data. For the purpose of information security, a collaborator is any individual or entity that has an established Business Associate Agreement (BAA) and Data Use Agreement (DUA) with MNCM.

Responsibilities of collaborators include the following:

Adhere to Established BAA and DUA Requirements
The purpose of a BAA and DUA is to set forth the terms and conditions pursuant to which a Collaborator may submit or receive certain data from MNCM through MNCM's data collection solution. The BAA and DUA also covers project specifics in regard to breach notification, security requirements, and Collaborator data requirements. Each collaborator should review their existing BAA and DUA with MNCM.

Report actual or suspected security violations or breaches to MNCM Security

A security incident is any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information. This includes interference with information technology operation and violation of MNCM policy, laws, or regulations. It is important that actual or suspected security incidents are reported as early as possible so that MNCM can limit the damage and scope of the reported incident.

How to report a security incident
email: security@mncm.org
phone: 612-455-2911