

**City of Minneapolis**  
**Policy for**  
**Enterprise Information Management**

---

**Origin:**

Developed by the City Clerk's Office and Business Information Services.  
Based on requirements set forth in Federal and State regulations and best practices developed by other governments.

**Approval Dates:**

Department Head Approval: July 29, 2003  
City Council Approval: August 22, 2003

**Authority:**

This policy applies to all employees under the jurisdiction of the City Council

**Contacts:**

Bill Beck	Business Information Services	673-2572
Casey Carl	City Records Manager	673-3765

---

# **EIM Policy**

## **Table of Contents**

Policy Preface.....	1
Enterprise Information Management Policy.....	2
Policy Requirements.....	3
Governance.....	3
Managing Information.....	3
Maintaining Public Trust.....	5
Additional Considerations Related to Electronic Media.....	5
Responsibilities.....	6
EIM Policy Board.....	6
EIM Project Sponsors.....	7
City Records Manager.....	7
Manager, Enterprise Data Management.....	8
Program Managers, Business Analysts and Subject Matter Experts.....	8
Department Heads.....	9
All Employees.....	9
Monitoring and Compliance.....	9
Appendixes.....	10
Appendix A - Authorities/Legal Framework.....	10
Appendix B - Glossary of EIM Project Management Terms.....	14
Appendix C – Glossary of Information Management Terms.....	15

# City of Minneapolis

## Enterprise Information Management (EIM) Policy

### Policy Preface

Enterprise Information Management is a program that is designed to create a standardized governance framework of policies, procedures and application tools for the life cycle management of electronic information resources across the enterprise. The EIM Policy provides guidance for managing City information in a comprehensive and strategic manner and sets boundaries and establishes the direction for the EIM program.

This document includes the EIM Policy and EIM Policy Requirements. The EIM Policy includes statements that identify how the City will manage its information. The EIM Policy Requirements outline the activities necessary to implement the policy. The EIM Policy can be viewed as an umbrella policy that will eventually include more specific policies that will bring together EIM components (records retention, data practices, stewardship, storage, security, etc.). The supporting policies will provide the specific details and guidance necessary to build the EIM infrastructure for the City.

The EIM Policy provides guidance for building enterprise information integrity by providing direction for meeting legal and regulatory mandates; identifying evidentiary requirements; and addressing the accountability requirements for the governance and stewardship of information. The policy mandates the inclusion of EIM requirements into strategic planning processes and the early integration of requirements during business process analysis and business systems implementation. The policy aligns with City Goals and supports the access to information in accordance with the Minnesota Government Data Practices Act and the retention of records in accordance with the Records Management Act.

The EIM Policy includes the concept of information life cycle by directing the management of information through its existence. The life cycle of information encompasses stages from creation and collection of the information to maintenance, access, use, storage, and disposal (or preservation). The life cycle concept is important to include in the EIM Policy for several reasons. Today, almost 70% of all City business transactions are electronically based and are never reduced to paper form. Many of the records required to provide evidence of City business transactions require a much longer life than the technology that supports it. Information can be requested at any point in the life cycle and therefore must be managed and accessible for as long as the information is required. In addition, privacy protection must be able to be applied or released at any point from the creation to the destruction of the information. For these and for a variety of other reasons, the City and its employees need to understand the importance of information lifecycle activities and learn how to effectively apply and integrate them in the daily operation of business.

## **Enterprise Information Management Policy**

The City of Minneapolis will provide the governance structure necessary to implement business systems that will effectively manage information throughout its life cycle. The City will deploy business systems that produce and manage information that is trustworthy, creates essential evidence of business transactions, meets required legal and regulatory mandates and utilizes industry best practices.

### **The City of Minneapolis will:**

- A. ensure that governance and accountability structures are implemented for the management of information under its control and in support of effective decision-making; and
- B. integrate information management requirements into the development of new, modified and existing systems and programs and include information management requirements into the annual department strategic planning process; and
- C. create records of business transactions required to document City programs and services subject to legal and regulatory requirements; and
- D. manage information regardless of medium or format in a manner that retains its quality, authenticity and integrity for as long as it is required; and
- E. ensure information that is created and received is accessible and is understandable, usable and can be disseminated throughout its life cycle; and
- F. ensure information is effectively organized for retrieval throughout its life cycle; and
- G. ensure information is effectively stored, maintained and protected throughout its life cycle; and
- H. ensure information is properly disposed of or preserved throughout its life cycle; and
- I. protect private information and provide timely access to public information; and
- J. provide sufficient security for information to mitigate risks associated with the use of and the transmission of electronic information; and
- K. ensure City elected officials and staff understand and share the responsibility for managing information as data stewards; and
- L. monitor the compliance of information management requirements.

## **Policy Requirements**

The Policy Requirements provide the direction as to what must be done to implement the policy. The Policy Requirements support the EIM Policy by providing guidance on the integration of information management activities into operational processes. The integration will facilitate policy implementation and more effective service delivery. The EIM Policy Requirements include; Governance, Managing Information, Maintaining Public Trust and Additional Considerations Related to Electronic Media.

### **1. Governance**

The EIM Policy Board, Business Information Services (BIS) and the Records Management Division of the City Clerk's Office will provide the leadership for the EIM Program and activities required to achieve this policy.

#### **1.1 To ensure accountability, the City will:**

- A. create an EIM Policy Board which has the responsibility and accountability for implementation of this policy and for the promotion of good information management and access principles;
- B. provide direction in the establishment of a framework of policies, procedures, best practices and toolkits for the application of and governance of the EIM program;
- C. include information management requirements as an integral part of the BIS system project proposal and planning process;
- D. provide direction in the development of training programs and tools to support City employees in managing information in the conduct of their activities;
- E. provide management and oversight to strategically integrate technologies and infrastructure to effectively support the management of information;
- F. develop formal agreements to document stewardship and accountabilities for sharing information between lines of business at the City and when entering into collaborative arrangements with other government entities and/or non-governmental organizations;
- G. create a process of periodic evaluations and initial audits to monitor compliance of information management requirements.

### **2. Managing Information**

The City will manage information throughout the life cycle of the information and develop an information management program to deliver effective and accessible information, programs and services. Information under the control of the City will be effectively managed regardless of medium or format.

**2.1 To ensure effective information management, the City will:**

- A. implement a program for information management that will include, at a minimum, strategic plans and priorities;
  - (1) include information management requirements at an early stage in the development of new or modified activities, programs, services and systems;
  - (2) integrate information management into current activities, programs, services and systems;
  - (3) optimize the use of existing information and make plans for its use beyond immediate business needs;

**2.2 To ensure that information is created, received and/or captured to provide evidence of business transactions and to ensure that the information is available and usable throughout its life cycle, the City will:**

- A. identify information management accountability requirements in policies, and implement the policies in programs, services and products;
- B. for each business process, identify the records that need to be created and managed to provide evidence of business transactions and decisions to account for City operations;
- C. identify the long term and vital records that are required to ensure continuity in the management of enterprise systems; and

**2.3 To ensure that information is effectively organized and is accessible throughout its life cycle, the City will:**

- A. provide an effective means for identification and retrieval of information by developing classification schemes or other systems to establish a coordinated approach for describing the enterprise's information assets;
- B. ensure appropriate dissemination/publication of information subject to legal and policy obligations;
- C. provide secure and timely access to information by the public, employees and other government entities and partners; and

**2.4 To ensure that information is effectively stored, maintained and protected throughout its life cycle, the City will:**

- A. develop trustworthy systems that produce trustworthy and reliable evidence of business transactions and ensure the availability of information over time and through changes in technology;
- B. develop procedures to ensure the security of private or other protected information for as long as it is required; and

**2.5 To ensure that information is effectively disposed of or preserved, the City will:**

- A. inventory the City's information assets to identify records required to provide evidence of business transactions and to meet legal and regulatory requirements;
- B. develop retention and disposition schedules and develop procedures for monitoring and reporting compliance;
- C. dispose of information according to State approved retention schedules; and
- D. ensure the preservation of historical information and the reliable access to information of enduring value.

**3.0 Maintaining Public Trust**

The City is committed to responding to the information needs of citizens and serving the public interest. The public expects government information and services to be complete and easy to understand and use. They also expect the City to provide affordable and cost-effective information, programs and services and safeguards for protecting and preserving the information appropriately.

**3.1 To deliver effective and accessible information, programs and services the City will implement systems that will:**

- A. organize information to provide clarity, context and access to information and services for the public;
- B. ensure the quality and consistency of information;
- C. create the required records to provide evidence of business transactions and decisions;
- D. ensure appropriate security and protection of private and protected information;
- E. promote efficiencies by re-using and sharing information;
- F. ensure the availability of information for the time periods required by law.

**4.0 Additional Considerations Related to Electronic Information**

The City is committed to doing business electronically and using technology as a means to enhance program and service delivery. New technologies create new information management challenges and opportunities particularly as they relate to the efficient, secure and timely access to information over time and through changes in technology.

#### **4.1 To support this commitment, the City will:**

- A. integrate records management and data practices requirements into systems that are used to create and manage electronic information;
- B. develop recordkeeping metadata requirements to describe information in electronic media in order to provide context, easy access/retrieval and provide access over time and through changes in technology;
- C. implement security methods to mitigate risks associated with the use of and transmission of information on electronic information systems and to ensure that private and other protected information is secure for as long as it is required;
- D. develop accountability requirements (stewardship) and control mechanisms to ensure the trustworthiness of electronic information;
- E. design systems that maximize opportunities for common data and system infrastructures to optimize data sharing; reuse; and systems interoperability where possible.

#### **5.0 Responsibilities**

City officials and staff are responsible for managing information throughout its life cycle in the performance of their duties.

#### **5.1 EIM Policy Board**

The EIM Policy Board establishes the goals and priorities for the EIM Program and develops and approves policy recommendations for information management for the City. The EIM Board makes decisions on structure, projects, resource commitments and educational activities on behalf of the City to develop and accomplish the EIM goals.

Responsibilities of the EIM Board include:

- A. ensuring implementation of this policy and creating a culture that supports the value of information management;
- B. designating workgroups and subject matter experts to address policy issues and create products to identify, address and help to resolve information management issues;
- C. approving formal agreements with recipient organizations when information is being transferred to other jurisdictions or the private sector;

- D. collaboration with the EIM Project Sponsors in identifying and developing City-wide goals and practices consistent with promoting information management practices within the City.

## **5.2 EIM Project Sponsors - City Clerk's Office and Business Information Services**

Working together, the City Clerk's Office (City Clerk) and Business Information Services (Chief Information Officer) will ensure that the City's Goals, Strategic Planning and Department Business Plans address information management needs including; data practices, information and data sharing, retention and other high-level information management requirements. They are responsible for organizing and leading the ongoing development of Citywide information management policy, required architecture and identifying the information and data management responsibilities required to support department strategic plans.

Responsibilities of the EIM Project Sponsors include:

- A. designing and implementing information management plans, systems, procedures, standards and guidelines in conjunction with program managers, business analysts and subject matter experts;
- B. developing and implementing accountability frameworks for collaborative arrangements pertaining to initiatives where information is being shared with other lines of business, other government entities or non-government organizations;
- C. assessing resource and training requirements needed to support information management functions and activities;
- D. monitoring and evaluating the efficiency and effectiveness of the information management plans, systems, procedures, standards and guidelines in collaboration with program managers and subject matter experts.

## **5.3 City Records Manager**

Under the City of Minneapolis Records Management Policy (1998), the Records Manager has specific roles and responsibilities related to the management of City records, which include:

- A. creating records retention schedules to enable City departments to dispose of records, or allowing for their transfer to the City Archives;
- B. providing direction and assistance in planning the retention and disposal of City records;

- C. assisting in the development of operational policies, tools and guidance in support of City-wide and department-specific information management programs;
- D. assuming a leadership role in the EIM program and serving as an authoritative source on policies, systems, methods, standards and practices for the management of records of the City of Minneapolis;
- E. directing the City's compliance with the Minnesota Government Data Practices Act in the role as the City's Responsible Authority;
- F. providing direction in Data Practices classification of information;
- G. protecting private information and facilitating access to public information.

### **5.3 Manager of Enterprise Data Management**

The responsibilities of Enterprise Data Management staff include:

- A. providing technical support and advice to the EIM Policy Board;
- B. work with EIM staff to establish workflow, communication and accountability structures necessary for providing analysis, direction and requirements during project planning and implementation;
- C. implement EIM directives into development standards for all new development activities;
- D. identify business requirements and application functional deficits with respect to EIM policies;
- E. align City BIS architectural and strategic direction with the EIM policy initiatives as they become available; and
- F. develop and implement a master plan to retrofit EIM standards into existing applications

### **5.4 Program Managers, Business Analysts and Subject Matter Experts**

Responsibilities of program managers, business analysts and subject matter experts include:

- A. identifying information requirements required to support systems planning and design and the development of information management procedures, standards and guidelines;
- B. ensuring adherence to information management procedures and standards in the conduct of business activities;
- C. collaborating with Project Sponsors in monitoring the efficiency and effectiveness of information management plans and activities.

## **5.5 City Department Head Responsibilities**

Responsibilities for managing City information include:

- A. representing their departments for the purposes of this policy;
- B. ensuring the integration of information management requirements into Department Business Plans and other strategic planning activities;
- C. approve and direct the assistance of staff during systems design to ensure that information management requirements are met;
- D. ensuring the integration of records management requirements (retention, data practices, records creation, etc) for all information (paper and electronic) into department business functions;
- E. ensuring the compliance of data stewardship requirements (information management accountability structure);
- F. ensuring the support of training and development programs for staff;
- G. ensuring that information management functions are periodically evaluated and audited for compliance with this policy.

## **5.6 All Employees**

All employees are responsible for creating and managing records that document business transactions and decisions and applying information management principles, standards and practices in the performance of their duties.

## **6.0 Monitoring and Compliance**

The City will assess the effectiveness and degree of compliance in meeting the requirements of this policy through periodic evaluations and internal reviews. The EIM Policy Board will use the reviews of departments and business functions to monitor compliance with all aspects of this policy.

## **7.0 Appendices**

Appendix A – Authorities and Legal Framework  
Appendix B – Glossary of EIM Project Management Terms  
Appendix C – Glossary of Information Management Terms

## **Appendix A Information Management Legal Framework**

### **Legal Authorities**

This policy is issued under the authority of the Information Policy Board, the Records Management Act and the Minnesota Government Data Practices Act.

### **Information Management Legal Framework**

Understanding existing regulations that affects the EIM program is important to the development of policy, procedures, best practices for department use. Data, information, records and information systems are subject to specific Minnesota statutes and Federal legislation, including general records laws and electronic records laws. In addition to the laws listed below, there are approximately 1800 regulations that affect the retention of specific records that are created and managed by the City. This listing is available from the City Clerk Records Management Division.

#### **A. Minnesota general records laws include:**

- Official Records Act (Minnesota Statutes, Chapter 15.17) (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>)
- Records Management Act (Minnesota Statutes, Chapter 138.17) (available at <http://www.revisor.leg.state.mn.us/stats/138/17.html>)
- Minnesota Government Data Practices Act (MGDPA) (Minnesota Statutes, Chapter 13) <http://www.revisor.leg.state.mn.us/stats/13>)

#### **B. Electronic records laws include:**

- Uniform Electronic Transactions Act (UETA) (Minnesota Statutes, Chapter 325L) (available at: <http://www.revisor.leg.state.mn.us/forms/getstatchap.shtml>)
- Electronic Signatures in Global and National Commerce (E-Sign), a federal law. (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>)
- Minnesota Recordkeeping Metadata Standard IRM 20 (Minnesota Historical Society) (available at: <http://www.mnhs.org/preserve/records/metadastandard.html>)
- Trustworthy Information Systems (guideline) (Minnesota Historical Society) (available at: <http://www.mnhs.org/preserve/records/tis/tis.html>)

#### **C. Federal legislation affecting E-Government initiatives include:**

- Clinger-Cohen Act (CCA)
- Government Paper Elimination Act (GPEA)
- Government Information Security Reform Act (GISRA)
- Sarbanes Oxley Act
- OMB Circular A-130 Management of Federal Information Resources

- Health Insurance Portability and Accountability Act (HIPAA), (P.L. 104-191)

**D. Official Records Act** -The Official Records Act is a general records law that mandates that "all officers and agencies" at all levels of government "shall make and preserve all records necessary to a full and accurate knowledge of their activities." This mandate reflects a concern for accountability: since government spends public money on public services, government agencies must be accountable to citizens, government administrators, courts, the legislature, financial auditors, and to history—that is, to future generations. Under the Official Records Act, the City's chief administrative officer is responsible for creating and preserving government records, including electronic records. This statute also allows records to be copied to another format or storage medium and still preserve the authenticity, reliability, and legal admissibility of the record, as long as the copies are made in a trustworthy process.

**E. Records Management Act** - The Records Management Act recognizes that creating comprehensive records and preserving them forever would be an impossibly expensive burden. Instead, the Act creates a mechanism for the orderly and accountable disposition of records in the form of the Records Disposition Panel. The Act also makes the state's Department of Administration (the Information Policy Analysis Division specifically) responsible for overseeing the records management process. The Records Disposition Panel includes the Attorney General, for expertise on the legal value of records; Director of the Minnesota Historical Society, for expertise on the historical value of records; and State Auditor (for local agencies), for expertise on the accounting value of records. The panel reviews, evaluates, and approves or disapproves requests to dispose of records, to transfer records, and to establish records retention schedules.

**F. Minnesota Government Data Practices Act** - The MGDPA assumes that government records (including electronic records) should be accessible to the public. Citizens should know what the government is doing, because the government must be accountable to the public. However, government agencies create some records that are confidential or private, such as medical records. So, while in theory all records are presumed to be publicly accessible, many exceptions exist. Only the Minnesota state legislature defines these exceptions. Any organization, public or private, that improperly releases data covered by the act could suffer significant penalties.

**G. Uniform Electronic Transactions Act and Electronic Signatures in Global and National Commerce** - UETA and E-Sign were both enacted in 2000. Both laws intend to facilitate the use of information technology in government and business by addressing the legal obstacles that exist in a system oriented towards paper records and signatures.

The primary message of the laws is that a court may not determine that an electronic record or signature is untrustworthy simply because it is in an

electronic format. A court can, though, reject electronic records and signatures because a government agency is creating, using, or managing them in an untrustworthy system or manner. One indicator of untrustworthiness would be an agency's failure to respect the laws governing records.

**H. Clinger-Cohen Act** - The Act seeks to increase the responsibility and accountability of departments and agencies in achieving substantial improvements in the delivery of services to the public and in other program activities through the use of modern information technology. The Act also facilitates and provides for the efficient and effective use of modern information technology.

**I. The Government Paper Elimination Act** - (GPEA) specifically provides for Federal agencies, by October 21, 2003, to give the public the option to submit information electronically; to maintain or disclose information to the public using electronic means; and to use electronic authentication methods to verify the identity of the sender and the integrity of electronic content. The law directs agencies to engage in the "acquisition and use of information technology, including alternative information technologies that provide for electronic submission, maintenance, or disclosure of information as a substitute for paper, and for the use and acceptance of electronic signatures."

**J. The Government Information Security Reform Act (GISRA)** - Requires Federal Agencies to assess the security of their non-classified information systems. More important from an enforcement perspective the law requires every agency to provide a risk assessment and report of the security needs of its systems. All agency programs must include procedures for detecting, reporting and responding to security incidents, including notifying and consulting with law enforcement officials, other offices and authorities, and the General Services Administration's Federal Computer Incident Response Capability (FedCIRC).

**K. Sarbanes Oxley Act** - Sarbanes-Oxley imposes new safeguards (including records creation and retention requirements) on public accounting firms that want to audit publicly traded companies, publicly traded companies, and firms with securities analysis and investment banking functions. The Act also amends the U.S. Code dealing with obstruction of justice within the context of crimes.

**L. OMB Circular A-130 Management of Federal Information Resources** - Circular No. A-130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act. The Act also establishes a minimum set of controls to be included in Federal automated information security programs and assigns Federal agency responsibilities for the security of automated information.

**M. Health Insurance Portability and Accountability Act (HIPAA)** - HIPAA provides direction to improve the portability and continuity of health insurance coverage; to combat waste, fraud and abuse; to improve access to services and coverage; and to simplify the administration of health insurance. The US Department of Health and Human Services, created regulations establishing national standards for privacy of health information. The regulations: establish several basic rights for individuals with respect to their health information and place limits on the use and disclosure of health information.

**N. Other General Records Laws:**

- Americans with Disabilities Act of 1990 (42 U.S.C. 12101 et. seq.) and the Rehabilitation Act Amendments of 1992 (29 U.S.C. Section 794)
- Computer Security Act of 1987 (40 U.S.C. Section 759 et. seq.)
- Copyright Act of 1976 (Title 17, United States Code, Sections 101-810) and Copyright Basics, Circular 1, Copyright Office, Library of Congress, Washington, DC, January 1991
- Establishment of Government Information Locator Service OMB Bulletin No. 95-01
- Federal Depository Library Program (44 U.S.C. Section 1902)
- Federal Records Act (44 U.S.C. Chapters 29, 31, 33, 35), National Archives and Records Administration Regulations (36 CFR Chapter 12, Subchapter B, "Records Management")
- Freedom of Information Act (5 U.S.C. 552)
- Information Technology Management Reform Act of 1996 (40 U.S.C. Chapter 25), Executive Order 13011
- Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35), (February 20, 1996)
- Privacy Act of 1974 (5 U.S.C. Section 552a)

## **Appendix B**

### **Glossary of EIM Project Management Terms**

**Policy:** strategic guidance that sets boundaries, establishes direction, influences other decisions and prescribes conduct.

**Principles:** a statement of preferred direction or practice. Principles constitute the rules, constraints and behaviors that an organization will abide by in its daily activities over a long period of time.

**Procedures:** specific practices or requirements to be followed focusing on specific methods and identifying accountability.

**Standards:** specific and mandatory practices or requirements to be followed focusing on results and identifying accountability.

**Guidelines:** best practices, suggested approaches, or methods intended to provide the means of meeting requirements of policies or standards.

**Best Practices:** recommended methods that serve to direct or guide the detailed, design, selection, construction, implementation, deployment, support or management of a project or program. Best practices are based on the success stories of one or more organizations or the industry as a whole.

**Toolkits:** specific methodologies and “how to” tools (e.g. templates, checklists, forms, etc.) created for use by staff and the public for the management, planning, and delivery of information systems and City services in a manner consistent with the City Information Management Policy.

**Data Management:** Controlling, protecting, and facilitating access to data in order to provide users with timely access and the accurate data that they need.

**Information Management:** discipline that directs and supports effective and efficient management of information in the City, from planning and systems development to creation, use, storage, disposal and/or long term storage of the information.

**Enterprise Information:** Information that is defined for use across an entire environment (citywide). Enterprise information is often (but not always) maintained in a shared central repository, connected to disparate computer systems, which provides common management, protection and information sharing capabilities.

**Data Sharing/Integration:** The sharing of information between unrelated systems between organizations, providing a single point of interface to which applications and databases connect and the resolving of differences between systems.

## Appendix C Glossary of Information Management Terms

<p><b>Accessible</b></p>	<p>"Accessible" means information arranged, identified, indexed or maintained in a manner that permits the custodian of the public record to locate and retrieve the information in a readable format within a reasonable time.</p> <p>The term "accessible" means that the information system allows the City to find, obtain and retrieve the needed information from the system.</p> <p>The term "government data" means all data collected, created, received, maintained or disseminated regardless of its physical form, storage media or conditions of use.</p> <p>"Public data" means data, which is accessible to the public.</p> <p>"Private data" means data that is not public but is accessible to the individual subject of the data.</p> <p>"Confidential data" means data that is not public and is also not accessible to the individual subject of the data.</p> <p>The "Responsible Authority" for government data is defined in Minn. Statute 13.02 and Minn. Statute 13.05 as the person with certain legal responsibilities for determining whether or not to provide access to information under Minnesota Government Data Practices Act.</p> <p>"Designee" is defined as any person designated by the Responsible Authority to be in charge of individual files or systems containing government data and to receive and comply with requests for that data.</p> <p>"Reasonable time" is not defined in the law. The intent of this provision is for government agencies to address the need for timely retrieval of information, to meet government agency needs and also to anticipate and prepare to respond to public information requests.</p>
<p><b>Accurate</b></p>	<p>"Accurate" means all information produced exhibits a high degree of legibility and readability and correctly reflects the original record when displayed on a retrieval device or reproduced on paper.</p>
<p><b>Authentic</b></p>	<p>"Authentic" means the retained electronic record correctly reflects the creator's input and can be substantiated.</p> <p>Records Management Standard ISO 15489 explains the term "authentic" as follows:          "An authentic record is one that can be proven:          a) to be what it purports to be</p>

	<p>b) to have been created or sent by the person purported to have created or sent it</p> <p>c) to have been created or sent at the time purported.</p>
<b>Backup and Recovery</b>	"Backup and recovery" are methods designed as an integral part of all data storage systems that address the business requirements of the data regarding availability, accuracy, and timeliness of data.
<b>Content</b>	"Content" means the basic data, message or information carried in a record.
<b>Context</b>	"Context" means the relationship of the information to the business and technical environment in which it arises. "Context" can include, but is not limited to, such elements as: the origin of the record; date and time the record was created; identification of the record series to which the information belongs.
<b>Data Definition</b>	"Data definitions" are used to help manage data resources by ensuring integrity (without duplication), providing clarity of meaning, and making data accessible to those who need it through precise identification of the required data.
<b>Data Practices</b>	The primary state law that governs the privacy of records is the Minnesota Government Data Practices Act. Proper application of Data Practices facilitates the access or restriction to data as permitted and required by law, prevents/provides data sharing as required by law and provides rights for individuals who are the subject of data.
<b>Data Quality</b>	Appropriate "data quality" is essential to making good decisions. Users of data must know the quality of the data in order to weigh the information properly for decision making.
<b>Electronic Format</b>	"Electronic format" includes information created, generated, sent, communicated or stored in electrical, digital, magnetic, optical, electromagnetic or similar technological form.
<b>Information System</b>	"Information system" means a system for generating, sending, receiving, storing or otherwise processing data.
<b>Legible</b>	"Legible" means the quality of the letters, numbers or symbols can be positively and quickly identified to the exclusion of all other letters, numbers or symbols when displayed on a retrieval device or retrieved by device or reproduced on paper.
<b>Life Cycle</b>	<p>"Life cycle" means all phases of a record's existence: creation; active use; preservation and management through to disposition.</p> <p>"Disposition" includes permanent preservation as well as designation for destruction.</p>
<b>Meaning</b>	"Meaning" means a record carries its original content, context and structure throughout its life cycle.
<b>Metadata</b>	"Metadata" is the term used to describe the structure of information resources required to make data understandable, usable and shareable. Common deployment of data documentation schemes promotes data

	reusability, reliability and the possibility of sharing across the enterprise.
<b>Public records</b>	<p><i>"Public records"</i> "All cards, correspondence, disks, maps, memoranda, microfilm, papers, photographs, recordings, reports, tapes, writings and other data, information or documentary material, regardless of physical form or characteristics, storage media or condition 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....</p> <p>The term 'records' excludes data and information that does not become part of an official transaction, library and museum material made or acquired and kept solely for reference or exhibit purpose, extra copies of documents kept only for convenience of reference and stock of publications and process documents, and bond, coupons, or other obligations or evidence of indebtedness, the destruction or other disposition of which is governed by other laws"</p> <p>"Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form" (Minnesota Statutes, Section 325L.02).</p>
<b>Readable</b>	"Readable" means the quality of a group of letters, numbers or symbols is recognized as words, complete numbers or distinct symbols.
<b>Records Audit/Inventory</b>	The "records audit/inventory" identifies major business functions/processes and classifies and defines the record groupings that support these functions. The information is used to identify legal requirements (retention, data practices, access, etc.) and for identifying the responsibilities for managing the records.
<b>Records Management</b>	"Records management" is the process used to create and maintain accurate records, present evidence, provide historical documentation, provide efficient services and allow its actions to be reviewed and audited.
<b>Records Retention Schedule</b>	The "records retention schedule" is a plan for the management of records that identifies how long records should be maintained. The purpose of the retention schedule is to provide continuing authority to dispose of or transfer records for long-term archival storage.
<b>Reliable</b>	<p>"Reliable" means the electronic record produced correctly reflects the initial record each time the system is requested to produce that record.</p> <p>Reliable may also be considered as "trustworthy," meaning that the electronic records can be relied upon as evidence of transactions because certain standards have been followed in the creation of the records. Those standards should include:</p> <ul style="list-style-type: none"> <li>• The systems that generated the records are periodically checked for errors.</li> </ul>

	<ul style="list-style-type: none"> <li>• Procedures to protect the integrity of the data are in place.</li> <li>• Adequate measures are in place to prevent the loss of data.</li> <li>• The records are produced in the normal course of business.</li> <li>• Reliability of the computer program can be verified.</li> </ul>
<b>Structure</b>	“Structure” means the appearance or arrangement of the information in the record. “Structure” can include, but is not limited to, such elements as heading, body and form.
<b>Trustworthy Systems</b>	A “trustworthy information system” is a system that can produce reliable and authentic information and records. A trustworthy system must demonstrate that it accurately reflects and records the business processes it was designed to facilitate. A trustworthy system provides safeguards to protect data against accidental, unrecorded, or unauthorized change or distribution.
<b>Usable</b>	“Usable” in the context of a record means that it can be located, retrieved, presented and interpreted.