CHISAGO COUNTY
REMOVABLE MEDIA USE POLICY

I. PURPOSE

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to connect removable media to any infrastructure within Chisago County's internal network(s) or related technology infrastructure resources. This removable media policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.
- Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media.
- USB card readers that allow connectivity to a PC.
- PDAs, cell phone handsets, and smartphones with internal flash or hard drive-based memory that support a data storage function.
- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, irDA, Bluetooth, among others) or wired network access.

The overriding goal of this policy is to protect the integrity of the private and confidential data that resides within Chisago County's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently moved outside the enterprise network and/or the physical premises where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, violation of many state and federal laws rules or policies, and damage to the Counties public image. Therefore, all users employing removable media and/or USB-based technology to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

This policy addresses a range of threats to – or related to the use of – enterprise data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive County data is stolen and inappropriately used or sold by an employee.
Copyright	Software copied onto portable memory device could violate licensing.
Spyware	Spyware or tracking code enters the network via memory media.
Malware	Viruses, Trojans, Worms, and other threats could be introduced via external media.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft and privacy laws.

II. POLICY GUIDELINES

A. Applicability

This policy applies to all Chisago County employees, including full, part-time and temporary staff, contractors and other agents who utilize company-owned removable media and/or USB-based technology to store, back up, relocate or access any organization or client-specific data. Such access to County data is a privilege, not a right, and forms the basis of the trust Chisago County has built with its clients, partners and constituents. Consequently, employment at Chisago County does not automatically guarantee the initial and ongoing ability to use these devices within the enterprise technology environment. The addition of new hardware, software, and/or related components to provide additional USB-related connectivity within the county technology infrastructure will be managed by the MICS Department. Non-sanctioned use of USB-based hardware, software, and/or related components to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy does not apply to such devices used in the MICS department for emergency or day to day management and repair of the County technology systems and networks. The MICS Department employees are provided with special, additional network and data security training as part of their employment with Chisago County that is not provided to any other county employees. This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of portable memory devices to any element of the enterprise network. If another policy, rule or law is more restrictive, the most restrictive policy, rule or law takes precedence.

B. Affected Technology

All USB-based devices and the USB ports used to access workstations and other related connectivity points within the county network will be centrally managed by MICS department and will utilize encryption and strong authentication measures. Failure to do so will result in immediate suspension of all network access privileges so as to protect the infrastructure.

It is the responsibility of any employee of Chisago County who is connecting a USB-based memory device to the technology infrastructure to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any portable memory that is used to conduct Chisago County business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

C. Procedures

The following procedures shall be followed:

1. Chisago County reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to the county technology infrastructure if it is determined that such equipment is being used in such a way that puts the technology infrastructure, data, users, and clients at risk.

2. All USB-related hardware and related software must be approved and purchased by the MICS Department only (no direct purchase of these devices from any supplier or vender by any other department is allowed).

3. The Chisago County MICS Department will maintain a list of approved USB-based memory devices and related software applications and utilities. Devices that are not on this list may not be purchased or connected to county technology infrastructure.

4. Employees using removable media and USB-related devices and related software for data storage, back up, transfer, or any other action within the county technology infrastructure will, without exception, use secure data management procedures. A simple password is insufficient. Employees agree to not disclose their passwords to anyone, particularly to family members if business work is conducted from home.

5. All USB-based devices or any type of removable media that is used for county business interests must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data.

6. Passwords and other highly confidential data are not to be stored on portable storage devices. End users must apply for new passwords every business/personal trip where county data is being utilized on USB-based memory devices.

7. Any USB-based or other memory device that is being used to store county data must adhere to the authentication requirements of Chisago County Electronic Data Policy. Employees, contractors, and temporary staff will follow all County-sanctioned data removal procedures to permanently erase data from devices once use is no longer required for business purposes.

8. Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function are not approved nor allowed devices for storage of any county data, or connection for any purpose to any county owned device or system.

9. End-users may not connect USB or other storage devices and media to the county technology infrastructure if the same has been connected to any non-county owned or controlled network infrastructure or devices. County data is not to be directly accessed on any system or equipment that is not owned and/or under the direct control of the County. The only exception to this would be "one time or one way use" media or devices, used for example, to transfer a power point presentation to a pc when giving a presentation. If a storage device / media is used on a non-county owned or controlled device, the device or media may not be reused or installed back onto any county system.

D. Policy Non-Compliance

Failure to comply with the Removable Media and Acceptable Use Policy may result in the suspension of any or all technology use and connectivity privileges as well as disciplinary action, up to and including termination of employment.