SECTION: RISK MANAGEMENT
TOPIC: PROPER USE OF IM EQUIPMENT & CONNECTIVITY
DATE: AUGUST, 2018

ADMINISTRATIVE PRACTICES MANUAL

SUBJECT: PROPER USE OF COMPUTER EQUIPMENT, SOFTWARE, and CONNECTIVITY

1.0 INTRODUCTION

It is the policy of Dane County for its employees to use the County's equipment, software and connectivity responsibly and ethically.

Part of responsible use of equipment, software and connectivity is the recognition that (a) storing data insecurely and/or sending data over insecure networks increases the risk of a data breach; and (b) data breaches often result in the loss of information, damage to critical applications, damage to the public. We do not want to impede business processes or increase expenses beyond what is necessary and prudent to provide appropriate controls that will prevent the loss of county information and ensure compliance with state and federal legislation and regulatory requirements.

Therefore, the following policy applies to all devices and accompanying media that stores Dane County data and/or connects to a Dane County network. This policy is complementary to Department-specific policies dealing with data access, data storage, data movement, and connectivity of devices to any element of the enterprise network; individual Departments may have more specific policies.

2.0 DUTIES OF INFORMATION MANAGEMENT

2.1. Information Management is responsible for managing the addition of new hardware, software, and/or related components that provide connectivity to Dane County networks. All devices attempting to connect to a Dane County network through the Internet may be inspected by Information Management. Devices that are not approved by Information Management, devices that are not in compliance with Information Management's security policies, and devices that represent any threat to the Dane County networks or Dane County data will not be allowed to connect.

2.2. Information Management will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion.

2.2.1. Information Management will encrypt hardware for all users that work with information regulated by:

- Internal Revenue Service (IRS)
- Gramm-Leach-Bliley Act (GLBA) Interagency Guidelines (also known as the Financial Modernization Act of 1999)

- Health Insurance Portability Act (HIPAA) Security Rule
- Criminal Justice Information Services (CJIS) Security Policy
- Other Statutes as required

2.2.2. Examples of information needing protection:

- ACH, EFT, credit card numbers, bank account numbers, PINS, and routing numbers are not to be stored on the County network;.
- Personal Health information
- Drivers license numbers
- PCI (Payment Card Industry) data
- County Employee home contact information such as SSNs and/or birthdates
- Law enforcement data, evidence, active investigations or active criminal proceedings, and PII related to undisclosed protection or investigative assignments

2.2.3. No one other than Information Management staff should purchase, install or download any software or applications that are not preapproved by Information Management.

2.2.4. No one other than Information Management staff should perform a factory reset of County owned equipment.

2.2.5. Information Management is responsible for accurately classifying the data in compliance with the FIPS 140-2 standard. The level of encryption on any removable media device will depend on the confidentiality requirement(s) of the data that will be put on the device After data classification, the following applies:

- Data not deemed "sensitive" is allowed to sit on the device unencrypted;
- The possibility of the presence of sensitive data on the device will mandate the use of encryption;
- If external regulation for the agency apply, the agency must comply with the stricter applicable regulation
- Information Management may restrict or disable any device deemed insecure;
- Information Management reserves the right to ban the use of any device at any time.
- Information Management can and will limit the ability of users to transfer data to and from specific resources on the County Enterprise network.

2.3. Information Management uses audit trails to track the attachment of an external device to the Dane County network, and the resulting reports may be used for investigation of possible breaches and/or misuse. Users of Dane County equipment and systems agree to

and accept that his or her use of Dane County owned equipment and/or connection to Dane County's networks may be monitored to record dates, times, duration of access, etc. Information Management may also use tracking applications (for example, "Find my iPad") on Dane County equipment.

2.4. If Information Management determines that equipment is being used in a way that puts the Dane County's systems, data, users, and/or clients at risk, then Information Management may disconnect (and/or refuse to connect) equipment to Dane County infrastructure.

3.0 DUTIES OF EMPLOYEES

3.1. Dane County equipment and systems should only be used to conduct official Dane County business. Personal use of Dane County equipment and data is governed by Dane County Ordinances.

3.2. Inappropriate use of Dane County equipment and systems includes, but is not limited to, conducting business for personal gain, political campaigning (including but not limited to any operations regarding collecting signatures and fundraising), visiting inappropriate websites, downloading inappropriate pictures and/or media files, and storing any digital media that has been illegally downloaded on County owned equipment. Users are responsible for understanding and complying with all copyright requirements related to digital media. To avoid inappropriate use of Dane County equipment, employees should not let friends and family use devices issued by Dane County Information Management..

3.3. Users must comply with Wisconsin's Open Records Law (see generally, Sec. 19.21 et seq. Wisconsin Statutes) and disclose data gathered using and/or stored on Dane County devices as required. There is no expectation of privacy when using County equipment or connectivity.

3.4. Users must comply with Wisconsin's Open Meetings Law (see generally Sec. 19.81 et seq. Wisconsin Statutes) and may not use email to decide matters before the County Board (see the Wisconsin Attorney General's January 25, 2010 informal opinion re the use of email to create a "walking quorum" http://www.doj.state.wi.us/sites/default/files/informal/20100125-jones.pdf).

3.5. Users are expected to secure equipment against being lost or stolen.

ADMINISTRATIVE PRACTICES MANUAL

3.5.1. Users are expected to use secure data management procedures such as strong passwords. Users should not share their passwords with anyone. Confidential data should not be stored un-encrypted on mobile devices.

3.5.2. In the event of a lost or stolen device, it is incumbent on the user to report the incident to Information Management immediately at helpdesk@countyofdane.com or (608) 266-4440. A device that has been lost or stolen can be remotely locked and wiped of all data to prevent access by anyone other than Information Management. If the device is recovered, it can be submitted to Information Management for re-provisioning.

3.6. Users are expected to secure data against being lost or stolen.

3.6.1. "Removable media" as that term is used in this policy includes:

- CD's, DVD's and floppy disks
- Portable USB-based memory sticks, also know as thumb drives, flash drives, jump drives, or key drives
- USB card readers that allow connectivity to a computer
- PDAs, smartphones with external flash or hard drive based memory that support storage functions
- Memory/SD cards or anything with flash-based (supplemental) storage media
- Portable music players (MP3 or MPEG players with internal flash or hard drive based memory that support storage functions
- Digital cameras with externa or internal memory
- Hardware that provides connectivity to USB storage via wired or wireless access.

3.6.2. Purchase of USB-based devices must go through Dane County Information Management.

3.6.3. Removable media may be used to distribute information to the public or other third parties if it has been classified for public access in terms of the Open Records Act and encryption is not required. Note that if encryption is required, then it is very likely that the information is not subject to release under Open Records.

3.6.4. Any non County-Owned devices used to synchronize with these devices must have anti-virus installed.

3.7. Users may not do anything to Dane County owned equipment that will permanently alter it in any way, including, but not limited to, exposing it to extreme temperatures or moisture. Users should clean LCD screens with a soft, dry anti-static cloth or with a screen cleaner designed specifically for LCD type screens. Users may not remove equipment's serial numbers or the label with Information Management's contact information.

3.8. Dane County staff should generally refrain from using devices (including but not limited to smartphones, laptops, and tablets) that are not owned by Dane County to perform County business. This policy is intended to safeguard staff's personal information, as well as information belonging to the County. Exceptions can be made for personal devices that follow regulatory compliance demanded by current applicable legislation and policy and as a privilege for an employee. Employees are put on notice that using personal devices for County business is completely voluntary and may make the devices subject to Open Records requests as well as loss of personal data resulting from wipe commands issued by Dane County Information Management.

3.9. All Dane County equipment must be returned to the issuing agency upon leaving office or employment. This includes mobile devices, chargers, keyboards, keyboard chargers and cases.

4.0 CONSEQUENCES FOR NON COMPLIANCE

4.1. Failure to comply with this Mobile Device Policy may result in the suspension of any or all technology use and connectivity privileges. In addition, an employee's failure to comply with this Policy may result in progressive discipline, up to and including termination of employment.

4.2. Dane County owned equipment is generally covered by warranties and insurance, but if Dane County owned equipment is lost or damaged due to neglect or abuse, it may become the user's financial responsibility to replace the equipment at current market price.

END OF POLICY