SECTION: RISK MANAGEMENT
TOPIC: PROPER USE OF COMPUTER EQUIPMENT & CONNECTIVITY
DATE: APRIL 2020

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 AND RIGHTS 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. Hardware: 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. Data: Information Management is responsible for accurately classifying the data in compliance with the FIPS 140-2 standard. Examples of information needing protection include:

- ACH, EFT, credit card numbers, bank account numbers, PINS, and routing numbers are not to be stored on the County network
- Personal Health information
- Driver's 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.

The level of protection 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.

2.2.3. Software: A standard suite of software is provided on all County computers to facilitate efficient support and compliance with copyright laws and license agreements.

- Only licensed and approved Dane County software will be supported by Information Management.
- The installation and use of personal software, including screen savers, on County computers is prohibited unless specifically authorized by the Division of Information Management.

2.3. 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. Occasional and limited personal use is acceptable, particularly in the case of emergencies.

3.2. Inappropriate use of Dane County equipment and systems includes, but is not limited to:

- Employees may not use County resources to conduct business for personal gain;
- Employees may not use County resources for political campaigning (including but not limited to any operations regarding collecting signatures and fundraising);
- Employees may not use County resources to visit inappropriate websites or download inappropriate pictures and/or media files;
- Employees may not use County resources to store digital media that has been illegally downloaded (employees are responsible for understanding and complying with all copyright requirements related to digital media);
- Employees may not use County resources to interfere with their own or another employee's work performance;
- Employees may not use County resources to disrupt service to the public;
- Employees may not use County resources to denigrate the credibility of the County or its officials or employees;
- Employees may not use County resources in a manner that interferes with the County's contractual relationships and/or contractual obligations

3.3. Other Restrictions

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

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

- 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.

- To avoid inappropriate use of Dane County equipment, employees should not let friends and family use devices issued by Dane County Information Management.

- 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.

- 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.

- 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.

3.4. Email Signatures. Employees' email signatures help to ensure that each official County email meets professional standards, represents the quality of our work and provides relevant information to the public. Therefore, employees' email signatures should follow the following guidelines:

- Employees may include their name, job title, department, mailing address, telephone number, fax number (if applicable) and the County or County Department's web address in their email signatures. Professional titles and certifications (such as PE for Professional Engineer or RN for Registered Nurse) may be listed after employees' names;
- While the official Dane County seal, Department-specific logos and approved graphics (for example, some Departments may promote participation in the

Census and Public Health promotes annual flu shots) are allowed, employees may not use non-Dane County logos, images, icons or clip art in their email; and

- While Department-specific taglines/slogans (such as "Conservation for Generations" for the zoo and "Fly Local" for the airport) are allowed, employees may not use personal or favorite quotes or epigraphs in their email signatures.
- Only personal pictures of the employee may be used; avatars or other images of an employee are not permitted. Employee pictures should be of a professional nature and should not be used to promote organizations or political campaigns or otherwise be incompatible with public service as that phrase is defined at 18.18 of the Dane County Ordinances.

3.5. 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.

3.6. 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.

3.7. Access is granted to individual users. To maintain security and accountability, passphrases, codes, and user names are the means by which access is granted to each individual user. Therefore, individual users are expected:

- To use strong passphrases with a minimum of 16 characters
- Not to share username or passphrase with anyone;
- Not to use someone else's username or passphrase to gain access;
- Limit access to properly authorized individuals by verifying that any individual doing computer maintenance is authorized to do so.

3.8. Data: Users are expected to secure data against being lost or stolen.

3.8.1. Devices used for "removable data" 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. Purchase of devices for "removable data" must go through Dane County Information Management "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.

3.8.2. Personal Devices. Employees are put on notice that using personal devices for County business is completely voluntary and doing so may make their personal devices subject to Open Records requests as well as loss of personal data resulting from wipe commands issued by Dane County Information Management.

Dane County offers the option for county employees to sync their county email, contacts, and calendars to their personal Android or iPhone devices. Due to the many different variations of Android devices, each device is configured differently and, therefore, specific instructions to setup a device cannot be made. If an employee has trouble setting up their personal device, Information Management will not be able to assist the employee and the employee will need to contact their service provider for assistance. However, the general information needed to setup a device is listed below.

- Setup differs from device to device but active sync has been known to work on many Android and iPhone/iPad devices.

- Information Management recommends using Microsoft Outlook as the preferred email app. It is available for download from the Apple App Store and Google Play Store.

- When creating a new account you'll want to select a Microsoft Exchange or Corporate account depending on the device.

  Server: mail.countyofdane.com (if needed)
  Domain Name: DC-NT-Domain (if needed)
  Username: Your county username
  Password: Password for your county account.

.

3.8.3. Any non County-owned devices used to synchronize with County data must have anti-virus installed.

3.8.4. This policy is intended to safeguard staff's personal information, as well as information belonging to the County.

3.8.5. Information Management does not have the resources to support personal devices for county employees. Therefore, 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.

3.8.6. 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.

4.0 CONSEQUENCES FOR NON COMPLIANCE

4.1. Failure to comply with this 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