Administrative Practices Manual

Subject: **IT Systems Risk Assessment Policy**

1. Purpose

Dane County Information Management (referenced as DCIM) is responsible for the overall compliance with IT best practices and standards to provide a secure IT environment while being considerate of costs. In accordance with these goals, DCIM must classify data stored within its IT network and through the use of various tools assess the security of this data.

2. Procedure for Identifying Data

2.1. DCIM shall setup secured data storage locations for department's use through a combination of Network Attached Storage (NAS), database, applications, secured government cloud or other available options based on best security practices for storing data.

2.2. It is the responsibility of departments to notify DCIM of new data storage requirement needs so that data can be classified and backed up in a secured environment. Departments shall not utilize the use of cloud-based systems (such as Google Drive or Dropbox) for business related purposes without the expressed permission of DCIM.

2.3. DCIM is responsible for securing data stored with appropriate role-based authentication controls.

2.3.1. Departments will identify DCIM Departmental Security Contacts that DCIM will work with to apply updated security roles to access this data and adjust permissions as needed.

2.3.2. DCIM may require departmental security forms to be updated on a regular basis as determined by DCIM for access to secured data

2.3.3. DCIM will secure this data, including Private Personal Information (PPI), Payment Card Industry (PCI), Protected Health Information (PHI) or Health Insurance Portability and Accountability Act (HIPAA), etc., in accordance with Federal and State regulations.

2.4. DCIM will be responsible for documenting and reporting security controls to the Director of Administration through an annual report submitted at the end of each calendar year.

2.4.1. The report shall include specific information on current tools used to secure the Dane County network and data, security events consisting of a "major" or higher impact, and an overall detailed network map.

2.4.2. This report can be shared with interested stakeholders per the discretion of either the DCIM Chief Information Officer or the Director of Administration.

2.4.3. Due to the sensitive data included in this report, it shall be marked as confidential and not shared without prior approval. DCIM will work with Risk Management and Corporation Counsel on redacting items of this report if needed

3. Proactive Security

3.1. DCIM is responsible for the regular scanning of all secured data storage locations and the overall network through the use of multiple automated tools.

3.2. Tools used to scan this data shall provide regular reporting to DCIM staff identifying when flagged data is stored – data such as Private Personal Information (PPI). DCIM will work with departments to determine if any data is to be moved to a more appropriate data storage location to limit access to only those who need it for their job duties.

3.3. DCIM will regularly perform tests on its systems and data storage locations to verify that automated scanning tools are detecting changes and the appropriate procedures are being followed to mediate those changes.
3.4. DCIM will subscribe to multiple sources of proactive security alerting services including private sector, local municipalities, state and federal partner organizations, to maintain awareness of security concerns and the ability to address them in a timely manner.
3.5. DCIM will actively engage with these partners, sharing non-classified information when appropriate.
3.6. DCIM will engage external third-party entities regularly to scan and assess vulnerabilities
    3.6.1. Real-time external monitoring of Dane County's network including weekly status reports.
    3.6.2. Multiple annual audits, including reviews from external vendors, will be completed on DCIM systems for specific departmental needs.
    3.6.3. Annual reviews will include recommended changes to DCIM procedures that are added to recurring meetings and will be included in the annual security report to the Director of Administration.
    3.6.4. DCIM will directly engage in a full external security audit of Information Technology systems no later than every 7 years

4. Compliance

All departments will work with DCIM to be in compliance with this policy. Exceptions to this policy will be approved by the Chief Information Officer and included in the annual report to the Director of Administration.