



Dane County IT Infrastructure

Dane County Information Management (DCIM) has two Direction Statements that help to govern the acquisition of hardware and software for the County:

1. Acquire hardware and software, which rank among the leaders in the industry, as balanced by their compatibility with the County's infrastructure, and by the resources needed for support.
2. Implement application software which meets our customers' needs, as balanced by their compatibility with the County's infrastructure, and by the resources needed for support.

To this end the DCIM has defined a mainstream set of hardware/software that are supported on the County network.

SUPPORTED SOFTWARE	
Server	DCIM operates primarily in a VMWare ESX virtual server environment in which all Microsoft and Linux servers along with virtual applications run as guest. When an option between Microsoft or Linux is available, Microsoft should be the default pick. Physical servers should be avoided unless justification is submitted and approved by DCIM. It is the expectation that any procured software can run within a virtual server environment.
User Authentication	DCIM runs a native Windows 2019 active directory domain as a primary directory service. Whenever possible it is the expectation that software applications should be integrated within active directory for authentication. 3 rd party applications would also be eligible to authenticate via SSO/SAML via Entra when available.
Email Integration	DCIM utilizes Microsoft Exchange 2019 as it's primarily supported email/messaging platform. Any applications or systems that require email connectivity or integration should interoperate with Microsoft Exchange 2019.
MDM Software	DCIM currently utilizes Meraki as an MDM solution.
Internet Browsing	DCIM supports applications that utilize Microsoft Edge or Google Chrome.
SQL	Microsoft SQL Server 2022 is the preferred backend DBMS for newly procured applications, however other DBMS platforms can be approved if on-going support is provided by the vendor. It is the preference of DCIM to not install stand-alone versions of SQL but instead use an SQL cluster connection for redundancy purposes. As needed, DCIM will procure SQL Standard licensing cores by default and Enterprise licensing cores when needed. These costs do not need to be included by the vendor and instead will be charged back to the department directly from DCIM.

SUPPORTED SOFTWARE (continued)	
Multi-user environment	DCIM operates primarily in a shared terminal services environment (Citrix). All software procured should work properly within this type of environment such as writing environmental values per user instead of device based.
Anti-Virus	DCIM utilizes Trend Micro (Apex One) software as a standard anti-virus protection client on all servers and workstations. Any exclusions that must be made to Trend for software to properly work must be provided to DCIM prior to implementation of services.
Remote Connectivity	DCIM provides external connectivity in the form of Citrix ICA client or software VPN as needed. This external connectivity is secured with two factor authentication provided by Entrust. Other non-persistent remote connectivity applications maybe permitted by DCIM with prior authorization on an as needed basis – connections made in this fashion will be disabled or uninstalled after each service window has been completed.
Camera Systems	See DCIM CCTV Standards for more detail. All Cameras shall be IP based.
Cloud Based Services	A service level agreement should be provided to DCIM by vendor that addresses the following topics. SLA must include expected up-time. Companies must provide information on the security measures they have in place that comply with PCI, SAS, NIST, HIPAA, CJIS or other security standards. Explanation of encryption to data – encryption levels used and if it is used in transit or at rest. Vendors must also provide information on where their data centers are located and what security measures are in place to separate data from other clients. Cloud vendors must provide certification that their staff that can access Dane County's data have based security backgrounds and provide information on what those security backgrounds entail. Data must be identified as owned by Dane County and written rules in place on how data will be exported and provided to Dane County in the event of a separation in business. Costs should be clearly listed out.

STORAGE	
NAS Systems	DCIM primarily uses Dell Unity with local storage for the handling of most user data. Access to this data is accomplished using iSCSI and/or Microsoft CIFS protocol as locally defined drives. It is the expectation that all software can properly communicate in an environment that utilizes non-local storage but rather redirected profiles on a NAS environment using SMB 3 or higher communication.
Backup	Data is replicated to a secured disaster recovery site utilizing replication software provide by Commvault. It is the expectation that any procured software will run the Commvault application so that proper backups of servers and SQL databases are resolved.

END USER DEVICES	
Workstations and Laptops	DCIM uses Lenovo workstations and laptops exclusively for all new deployments. Devices are deployed utilizing Windows 10 and the Microsoft Office 2021. Microsoft M365 is expected to be fully deployed by May 2025.
Thin Clients	DCIM utilizes Wyze Thin Stations exclusively for all new deployments.
Tablets	DCIM will attempt to support to the best of our ability any tablet that is County procured through the IT purchasing request process and has the most recent iOS or Android operating system installed. Tablets provided by a vendor as part of a project should receive on-going vendor maintenance and will not have standard internal network access. Devices that are setup by DCIM will have MDM software installed and may have limited network access.
Mobile Devices	DCIM will attempt to setup to the best of their ability any smart phone that is County procured and has the most recent iOS or Android operating system. Devices that are setup by DCIM will have MDM software installed and may have limited network access.
VoIP Phones	DCIM utilizes an extensive network of Mitel VoIP phones and controllers. Most workstations are setup to share a single Ethernet port between a VoIP phone and workstation device.

NETWORK INFRASTRUCTURE	
Networking	DCIM uses Dell hardware for all new network infrastructure. All equipment is expected to support software defined configuration. The primary network protocol used by DCIM is TCP/IP over Ethernet. Standard network speed to all workstations is 100 Mbps. The network backbone is connected via fiber-optic cable with 1 GBs and 10 GBs speeds. DCIM is removing Multimode fiber and changing to Singlemode in any new construction.
Wireless	DCIM utilizes Cisco controllers and AccessPoints to provide wireless connectivity throughout various county facilities. Internal network wireless access is available for DCIM managed devices at speed greater than 10 Mbps.
Server Applications	DCIM utilizes Citrix XenApps and Citrix XenDesktop as its primary application delivery methods. It is the expectation that all applications should work in this shared user environment.
Copper Telephone Lines	New applications and construction shall avoid the use of POTS lines where applicable. Cellular communication devices or communication over Ethernet are the preferred methods to replace POTS.

Below is a list of the most common standard hardware and software applications supported by DCIM that is requested for review of new products for compatibility.

HARDWARE	
Android Mobile Phones and Tablets	
Cisco Wireless Controllers and Access Points	
Citrix NetScaler Remote Access Appliances	
Dell Switches and Routers	
Dell Unity SAN	
Dell Power Edge Servers	
Lenovo Workstation	Minimum Specs Core i5 Processors, 8 GB RAM, 256 GB SSDs
Dell/Wyse Thin Clients	
HP MFP	Compatible with HP Digital Sending Software
HP Printers	
IOS (Apple) Mobile Phones and Tablets	
NetMotion Remote Access server	
OCE Plotters	
Ricoh MFP	