



DU PAGE COUNTY

Technology Committee

Final Summary

421 N. COUNTY FARM ROAD
WHEATON, IL 60187
www.dupagecounty.gov

Tuesday, April 1, 2025

11:00 AM

Room 3500B

1. CALL TO ORDER

11:00 AM meeting was called to order by Chair Covert at 11:12 AM.

2. ROLL CALL

PRESENT	Berlin, Chaplin, Childress, Covert, Eckhoff, Galassi, Henry, Kaczmarek, Lukas, Rutledge, and White
ABSENT	Yoo

3. CHAIRWOMAN'S REMARKS - CHAIR COVERT

Chair Covert encouraged everyone to complete the annual DuPage County Awareness and Usage AI survey. Additionally, she congratulated the IT Department Web Services team and the 18th Judicial Circuit Court for being named Smart Cities Awards finalists for their FVCC Domestic Violence QR Code Project.

4. PUBLIC COMMENT

No public comments were offered.

5. APPROVAL OF MINUTES

5.A. [25-0862](#)

Approval of Minutes for the Technology Committee - Regular Meeting - Tuesday, March 18, 2025

Attachments: [2025-03-18 Technology Minutes](#)

RESULT:	APPROVED
MOVER:	Sheila Rutledge
SECONDER:	Kari Galassi

6. RESOLUTIONS

6.A. [TE-R-0001-25](#)

Revision to the Technology Resources Acceptable Use Policy

Attachments: [EXHIBIT A - Policy 8.1 Technology Resources Acceptable Use Internet](#)
[Policy 8.1 Technology Resources Acceptable Use Internet - revised March 2025 Redline](#)
[AUP Changes Summary](#)

RESULT:	APPROVED AND SENT TO FINANCE
MOVER:	Sheila Rutledge
SECONDER:	Michael Childress
AYES:	Berlin, Chaplin, Childress, Covert, Eckhoff, Galassi, Henry, Lukas, Rutledge, and White
ABSENT:	Yoo
ABSTAIN:	Kaczmarek

7. PROCUREMENT REQUISITIONS

7.A. [TE-CO-0003-25](#)

Amendment to County Contract 6082-0001 SERV, issued to Dell, Inc., for a Microsoft Enterprise Agreement (EA) for all Microsoft Software and Azure Cloud Services for GIS and Information Technology, to increase the encumbrance by \$7,470, resulting in an amended contract total of \$3,857,514.05, an increase of 0.19%.

Mr. McPhearson explained that this change order is to add the purchase of Microsoft CoPilot AI licensing for use from now through 11/30/2025. He said the cost will increase some next year since this year is lower due to it not being a full year.

Member Henry asked what CoPilot does. Mr. McPhearson said it can help automate processes, obtain information faster, and make us more productive. Mr. Burnson added that it can do things such as take emails and create presentations based on the information collected.

Member White asked about potential issues with personal identifiable information (PII). Joe Hamlin, Network Systems Manager, responded that the Microsoft data loss prevention (DLP) will carry over to CoPilot.

Mr. McPhearson reinforced that we are purchasing these licenses to test CoPilot and develop policies moving forward.

Attachments: [Dell 6082-1-SERV - Change Order #5](#)
[Dell 6082-1-SERV - Change Order #5 - Decision Memo](#)
[Dell 6082-1-SERV - Change Order #5 - Quote #3000186576021.1](#)
[Dell 6082-1-SERV - Change Order #5 - VED](#)

RESULT:	APPROVED AND SENT TO FINANCE
MOVER:	Michael Childress
SECONDER:	Sheila Rutledge

8. TRAVEL REQUESTS

8.A. [25-0812](#)

Authorization for an IT staff member to attend the Tyler Connect 2025 Conference in San Antonio, TX from May 11, 2025 through May 14, 2025. Travel to include hotel, mileage, per diem, etc. for an estimated total of \$3,204.

Attachments: [Travel Request - Tyler Connect Conference](#)

RESULT:	APPROVED
MOVER:	Michael Childress
SECONDER:	Kari Galassi

9. INFORMATIONAL ITEMS

9.A. [JPS-R-0005-25](#)

Resolution to rescind JPS-P-0039-24, issued to Video and Sound Service, Inc., to provide maintenance and repair of the campus security system, as needed, for the County campus. (Contract total amount of \$301,582) (Office of Homeland Security and Emergency Management)

RESULT:	ACCEPTED AND PLACED ON FILE
MOVER:	Michael Childress
SECONDER:	Kari Galassi

10. IT PROJECT UPDATES

CIO Anthony McPhearson provided an update on IT projects, as attached hereto.

Chair Covert asked what the timeline is on the FOIA request tool. Mr. McPhearson said it will likely be toward the end of the calendar year.

[25-0966](#)

IT Project Updates Presentation

Attachments: [DuPage County Tech Committee Project Updates_4-01-25 Final.pdf](#)

RESULT:	PRESENTED
----------------	-----------

11. OLD BUSINESS

Chair Covert reminded committee members to raise their hands and be recognized for the record when speaking.

12. NEW BUSINESS

No new business was discussed.

13. ADJOURNMENT

With no further business, the meeting was adjourned.



Minutes

421 N. COUNTY FARM
ROAD
WHEATON, IL 60187
www.dupagecounty.gov

File #: 25-0862

Agenda Date: 4/1/2025

Agenda #: 5.A.



DU PAGE COUNTY

Technology Committee

Final Summary

421 N. COUNTY FARM ROAD
WHEATON, IL 60187
www.dupagecounty.gov

Tuesday, March 18, 2025

11:00 AM

Room 3500B

1. CALL TO ORDER

11:00 AM meeting was called to order by Chair Covert at 11:00 AM.

2. ROLL CALL

PRESENT	Berlin, Chaplin, Childress, Covert, Eckhoff, Henry, Kaczmarek, Rutledge, White, and Yoo
ABSENT	Galassi, and Lukas

3. CHAIRWOMAN'S REMARKS - CHAIR COVERT

Chair Covert remarked on the following items:

Ransomware Workshop - The IT department hosted a highly successful county-wide ransomware workshop on Wednesday, March 5, 2025. The hands-on, immersive tabletop exercise, co-hosted by our strategic vendor partner, Cohesity, and Michelle Amanti, DuPage County's Cybersecurity Engineer, was a testament to our collective efforts in making all our technology environments safer. It was a proud moment for us as several municipalities, agencies (such as OHSEM and ETSB), and departments, as well as IT staff, participated in the joint exercise.

GovAI Tool Demo and Municipal Use Case Workshop - This Friday, March 21, 2025, at 10:00 a.m., Debbie Deacy and Shanita Thompson, Co-Chairs of the AI Task Force, are hosting a GovAI tool demonstration and discussion on practical AI use cases for municipalities. This session will enable participants to observe an AI tool designed specifically for government organizations in action and discuss essential best practices for the safe and responsible adoption of AI in municipal operations. By the end of the session, participants will have a clear understanding of how AI can be leveraged to enhance municipal operations and the necessary precautions to ensure its safe and ethical use.

Smart Cities Awards Finalist - Congratulations to the IT Department's Debbie Deacy and Rhonda Brier and the 18th Judicial Circuit Court for being a Smart Cities Awards Finalist for the FVCC Domestic Violence QR Code Project! The winner will be announced soon, so let's wish them the best of luck.

4. PUBLIC COMMENT

No public comments were offered.

5. APPROVAL OF MINUTES

5.A. [25-0527](#)

Approval of Minutes for the Technology Committee - Regular Meeting - Tuesday, February 4, 2025

Attachments: [2025-02-04 Technology Minutes](#)

RESULT:	APPROVED
MOVER:	Michael Childress
SECONDER:	Yeena Yoo

6. PROCUREMENT REQUISITIONS

6.A. [TE-CO-0002-25](#)

Amendment to County Contract 6946-0001 SERV, issued to Insight Public Sector, for the replacement of backup appliances and annual maintenance and support of Veritas Netbackup software, for Information Technology, to increase the encumbrance by \$16,488.45, resulting in an amended contract total of \$391,207.29, an increase of 4.40%.

Mr. McPhearson advised the committee that staff is working on a retention policy to help save space and money, so the committee may see additional increases in this contract until a policy is in place.

Attachments: [Insight - 6946-1-SERV - Change Order #2](#)
[Insight - 6946-1-SERV - Change Order #2 - Quote #0228153423](#)
[Insight - 6946-1-SERV - Change Order 2 - Decision Memo](#)
[Insight - 6946-1-SERV - Change Order #2 - VED](#)

RESULT:	APPROVED AND SENT TO FINANCE
MOVER:	Yeena Yoo
SECONDER:	Michael Childress

6.B. [TE-P-0005-25](#)

Recommendation for the approval of a contract to Insight Public Sector, for the procurement of Okta Single Sign-On and Multifactor Authentication licensing, for Information Technology, for the period of April 30, 2025 through April 29, 2026, for a contract total amount of \$99,609.08. Contract pursuant to the Intergovernmental Cooperation Act (OMNIA Partners Cooperative Agreement #23-6692-03).

Attachments: [Insight \(Okta\) - PRCC](#)
[Insight \(Okta\) - Quote #0228141797](#)
[Insight \(Okta\) - Omnia Contract #23-6692-03](#)
[Insight - VED](#)

RESULT:	APPROVED AND SENT TO FINANCE
MOVER:	Michael Childress
SECONDER:	Sheila Rutledge

6.C. [25-0627](#)

Recommendation for the approval of a contract purchase order to Verizon Wireless, for wireless tablet and machine-to-machine services, for Information Technology, Department of Transportation, and Stormwater, for the period of February 1, 2025 to September 30, 2025, for a total contract amount not to exceed \$24,300, in compliance with Governmental Joint Purchasing ACT, 30 ILCS 525/2 (State of Illinois Master Contract #CMS793372P).

Attachments: [Verizon - PRCC](#)
[Verizon - State of Illinois Master Contract #CMS793372P](#)
[Department VED Placeholder.pdf](#)

RESULT:	APPROVED
MOVER:	Michael Childress
SECONDER:	Yeena Yoo

6.D. [25-0670](#)

Recommendation for the approval of a contract purchase order to SiteImprove, Inc., for annual web governance services, for Information Technology, for the period of May 1, 2025 through April 30, 2026, for a contract total amount of \$18,998.31. Per 55 ILCS 5/5-1022(d) exempt from bidding - IT/Telecom purchases which do not exceed \$35,000.

Attachments: [SiteImprove - PRCC](#)
[SiteImprove - Quote # S00004418-20250501](#)
[SiteImprove - VED](#)

RESULT:	APPROVED
MOVER:	Michael Childress
SECONDER:	Sheila Rutledge

7. **INFORMATIONAL ITEMS**

7.A. [JPS-CO-0002-25](#)

Amendment to Purchase Order 7357-0001 SERV, issued to Heartland Business Systems, to increase the contract encumbrance in the amount of \$23,213.20, for a new contract total not to exceed \$220,089.81, an increase of 11.79%. (Sheriff's Office)

Attachments: [Heartland-Change Order](#)
[Heartland-Decision Memo](#)
[Heartland-Vendor Ethics_Redacted](#)

RESULT:	INFORMATION RECEIVED AND PLACED ON FILE
MOVER:	Michael Childress
SECONDER:	Sheila Rutledge

7.B. [JPS-P-0016-25](#)

Recommendation for the approval of a contract purchase order to Flock Safety, to provide continuation of the Flock ALPR program, for the Sheriff's Office, for the period of March 1, 2025 through February 28, 2029, for a contract amount not to exceed \$777,602.74. Per 55 ILCS 5/5-1022 (c) not suitable for competitive bids. (Sole Source - No other vendors offer a similar service that is compatible with the existing cameras). (Sheriff's Office)

Attachments: [Flock Safety-PRCC](#)
 [Flock Safety-Quote](#)
 [Flock Safety-Sole Source](#)
 [Flock Safety-Vendor Ethics](#)

RESULT:	INFORMATION RECEIVED AND PLACED ON FILE
MOVER:	Michael Childress
SECONDER:	Sheila Rutledge

7.C. [JPS-P-0018-25](#)

Recommendation for the approval of a contract purchase order to West Publishing Corporation d/b/a Thomson Reuters-West, for the purchase of fifty (50) online passwords for Westlaw/Edge online legal research, for the period of April 1, 2025 through March 31, 2030, for a total contract amount not to exceed \$155,328. Per 55 ILCS 5/5-1022(c) not suitable for competitive bids - Sole Source. (18th Judicial Circuit Court)

Attachments: [West Publishing - PRCC Redacted.pdf](#)
 [West Publishing Order Form Online Signed Redacted.pdf](#)
 [West Publishing Sole Source Ltr Online.pdf](#)
 [West Publishing Vendor Ethics Signed Redacted.pdf](#)

RESULT:	INFORMATION RECEIVED AND PLACED ON FILE
MOVER:	Yeena Yoo
SECONDER:	Michael Childress

7.D. [25-0544](#)

Recommendation for the approval of a contract purchase order to Harris Govern, for annual software maintenance and support services, as needed, for the period of April 1, 2025 through December 31, 2025, for a contract total amount not to exceed \$15,891.75 (Building & Zoning - \$8,829, Division of Transportation - \$5,297.25, Public Works - \$1,765.50). Per 55 ILCS 5/5-1022(c) not suitable for competitive bids. (Sole Source - Support for Govern System.)

Attachments: [Harris Govern PRCC](#)
 [Harris Govern Invoice](#)
 [Harris Govern Sole Source](#)
 [Harris Govern Vendor Ethics](#)

RESULT:	INFORMATION RECEIVED AND PLACED ON FILE
MOVER:	Michael Childress
SECONDER:	Yeena Yoo

8. OLD BUSINESS

Member DeSart asked for additional information regarding item 7A, specifically if we buy passwords. Member Yoo stated they are necessary to access law databases. Member McCarthy added that they are for use in the law library, by the public, and possibly for judicial staff and judges. He noted that Suzanne Thompson can send more information.

9. NEW BUSINESS

No new business was discussed.

10. ADJOURNMENT

With no further business, the meeting was adjourned.



Technology Resolution

421 N. COUNTY FARM
ROAD
WHEATON, IL 60187
www.dupagecounty.gov

File #: TE-R-0001-25

Agenda Date: 4/1/2025

Agenda #: 6.A.

RESOLUTION
TO REVISE THE
DU PAGE COUNTY INFORMATION TECHNOLOGY
TECHNOLOGY RESOURCES ACCEPTABLE USE POLICY

WHEREAS, it is the practice of the DuPage County Board to provide employees with written policies;
and

WHEREAS, it is necessary to update and distribute guidelines for the Technology Resources
Acceptable Use Policy to employees under County Board jurisdiction; and

WHEREAS, it is the responsibility of the Information Technology Department to maintain and
distribute these policies; and

WHEREAS, the State's Attorney's Office has reviewed these policies.

NOW, THEREFORE, BE IT RESOLVED, that EXHIBIT A to this resolution be approved and adopted
by all departments under the jurisdiction of the County Board.

Enacted and approved this 8th day of April, 2025, at Wheaton, Illinois.

DEBORAH A. CONROY, CHAIR
DU PAGE COUNTY BOARD

Attest: _____

JEAN KACZMAREK, COUNTY CLERK



Policy 8.1	Technology Resources Acceptable Use		
<u>Effective Date:</u> 2/28/2012 <u>Last Amended Date:</u> 4/8/2025	<u>Applicable Law/Statute:</u> Illinois Information Security Improvement Act (20 ILCS 1375/5-30) Personal Information Protection Act (815 ILCS 530)	<u>Source Doc/Dept.:</u> None/IT	<u>Authorizing I.C. Sec:</u> None

TECHNOLOGY RESOURCES ACCEPTABLE USE

8.1

POLICY

DuPage County's policy is to provide employees with technology resources necessary to support our goals and objectives. This policy pertains to all technology-related equipment, hardware, and software, including, but not limited to County-owned, leased, or licensed desktop and laptop computers, tablets, telephones, cell phones, copy machines, fax machines, computer systems, e-mail, other messaging software, Intranet, and Internet services, tools, and supplies.

ELIGIBILITY

All employees under County Board jurisdiction, regardless of employment status. To the extent that this policy constitutes a term or condition of employment which is required to be bargained under any collective bargaining agreement, employees covered by such an agreement shall not be subject to the terms of this policy until such time as the bargaining agreement is amended or the policy terms are agreed to by the unit.

GUIDELINES

- A. The use of County technology resources is intended primarily for County business use; however, incidental and occasional use of these systems for non-work purposes may be permitted at the discretion of the Department Head under the following conditions:
 - a. Must not result in direct costs, cause legal action against, or negatively impact the County.
 - b. Must not interfere with the performance of work duties.
 - c. Must not cause a noticeable impact or change to operational infrastructure systems, noticeably consume resources, incur support, or otherwise

adversely affect the functioning of essential operations.

- d. DuPage County reserves the right to monitor personal use to ensure compliance with all policies and determine whether it is considered “Incidental Use” at the County’s sole discretion.
- B.** County employees shall have no expectation of privacy regarding their use of County technology resources. The County reserves the right to access any and all information, including files and e-mail stored on the County network or any County equipment. The County may at any time examine technology or information resources, or intercept, monitor, review, and share data with authorized personnel and law enforcement if necessary.
- C.** All County employees must use County technology resources in a manner that complies with applicable laws and policies. This includes adhering to the Freedom of Information Act, copyright and software licensing rules, property rights, and privacy protections. The County’s computer system must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Examples of this include:
- a. Copying and sharing images, music, movies, or other copyrighted material using P2P (peer to peer) file sharing, or unlicensed CD’s and DVD’s;
 - b. Posting or plagiarizing copyrighted material;
 - c. Downloading copyrighted files which the employee has not already legally procured;
 - d. Software without a valid license or from an unapproved source.
- D.** Employees are expected to exercise good judgement regarding appropriate use of County technology resources and equipment and adhere to any safety guidelines related to a piece of equipment.
- E.** Employees are expected to limit the use of personal electronic devices and other personal equipment for non-work-related purposes during working hours. Any limited use will be at the discretion of the Department Head.
- F.** Employees may not blog or use other forms of commonly known social media or technology, using County equipment on the Internet/intranet during their designated work schedule, unless specifically authorized by the Department Head as part of the employee's position.
- G.** DuPage County reserves the right to discontinue employee access to County equipment, if an employee is found to have posted content that is deemed inappropriate including, but not limited to, content which:
- a. Violates any laws;
 - b. Is libelous or may be construed as harassment (Personnel Policy 7.4: Harassment);
 - c. Violates any County policies, rules, standards, or requirements, including, but not limited to, the County’s Ethics Ordinance and Personnel Policy 9.1: Employment Ethics;

- d. Is averse to the reputation, interests, or business relationships of DuPage County.
- H. Instant messaging such as Microsoft Teams is allowed for County businesses communications only.
- I. Employees may not remove County equipment from the location where the equipment is assigned, except for cellular devices, equipment installed in vehicles, or equipment intended to be used in the field unless otherwise authorized by the Department Head and Information Technology. Once approved, Information Technology must be notified in order to update their records. Upon separation, all technology resources must be returned to the Information Technology Department.
- J. Employees shall not install, remove, or otherwise modify any hardware or software without written approval of their Department Head and Information Technology.
- K. Employees will be issued one desktop or laptop for their use. Employees will not be allowed multiple desktops or laptops for their sole use unless authorized by their Department Head and Information Technology. Kiosks or computers for use by multiple employees are exempt from this requirement.
- L. Employees are responsible for ensuring the protection and security of assigned County technology resources. Technology resources must be secured when not in use. Missing equipment must be reported to the Department Head, Security Department, and Information Technology immediately.
 - a. Laptop locks and cables must be used to secure laptops when in a non-secured area;
 - b. Mobile devices must be kept out of sight when not in use;
 - c. Care must be given when using or transporting devices in busy areas;
 - d. Generally, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.

NETWORK USE GUIDELINES

- A. The DuPage County Information Technology Department shall be the sole provider of designs, specifications, operations, maintenance, and management of all network infrastructure and equipment including, but not limited to, switches, routers, firewalls, wireless access points, and the wired/wireless local area network, except for departments that have their own network staff.
- B. With the exception of the Information Technology Department, and other employees approved by their Department Head and the Chief Information Officer (CIO), no employee shall be granted administrative rights to any network equipment.
- C. Remote access to the County systems shall only be allowed via County approved

software and hardware. Remote access systems are to be used in the same manner as computer systems within the County offices and are subject to the same policies. Employees shall ensure reasonable physical security is maintained for the computing systems used for remote access.

- D. Non-County provided equipment is expressly prohibited on the County's network.

COMPUTER USE GUIDELINES

- A. Employees must safeguard login identifiers and passwords. Any suspected password compromise must be reported immediately to the Information Technology Department. Password and access information may not be recorded, shared, or given to anyone other than the employee.
- B. No employee shall allow non-County Information Technology staff to assume unsupervised control of a computer or application to which you have logged in with your username.
- C. All employees are responsible for locking or logging out of their workstation before they leave the office/desk unattended.
- D. No employee shall be granted a primary login with administrative rights to their workstation, except as approved by their Department Head or the Chief Information Officer.
- E. No personal data shall be stored on County servers. This includes but is not limited to, documents, pictures, music, and video files. The Information Technology Department reserves the right to remove any personal documents, pictures, music, or video files without warning. Findings shall be reported to the employee's supervisor.
- F. No confidential information shall be stored on any local or removable media devices that are not encrypted with County approved encryption software.
- G. No County business-related data shall be stored on any local hard drives. The Information Technology Department will provide training to ensure that data is being stored in the correct location
- H. No County data shall be shared using non-County provided storage unless required by an outside vendor and with the approval of the Department Head.
- I. Employees are prohibited from modifying County-owned technology without approval from their Department Head and Information Technology Department. These modifications include, but are not limited to, software installation, hardware installation, and configuration changes. Installation of non-business-related software is prohibited.
- J. While the County permits limited personal Internet usage, the County assumes no responsibility for any content that the employee may view or read that they find offensive. The County may use software to filter offensive, sexually explicit, inappropriate, or non-business-related sites.

- K.** Streaming media, such as internet radio stations or internet videos, is allowed for job-related functions only, subject to the approval of the Department Head and/or Information Technology Department.
- L.** Excessive use, as defined by the Information Technology Department, of County bandwidth or other computer resources is not permitted. Bandwidth-intensive tasks that may degrade network capacity or performance such as large file downloads or uploads or streaming audio or video should be coordinated with the Information Technology Department. If contacted by the Information Technology Department with regards to the excessive use of bandwidth employees will follow the instructions of the Information Technology Department.
- M.** Utilizing county-owned or county-provided computer systems to bypass any established security, authentication, or user-access controls is strictly prohibited. Any deliberate attempt to circumvent these security measures, including efforts to escalate privileges, is expressly forbidden.
- N.** Illegal activities using County-owned or County-provided computer systems are prohibited. Such actions include but are not limited to:
 - a. Unauthorized port scanning, defined as systematically scanning a computer's ports;
 - b. Unauthorized network hacking, defined as any technical effort to manipulate the normal behavior of network connections and connected systems;
 - c. Unauthorized packet sniffing, defined as the act of capturing packets of data flowing across a computer network;
 - d. Unauthorized packet spoofing, defined as creating internet protocol packets with a false source IP address;
 - e. Unauthorized Denial of Services, defined as a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users;
 - f. Unauthorized wireless hacking, defined as accessing wireless networks by defeating the security devices within that wireless network;
 - g. Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system;
 - h. Acts of Terrorism;
 - i. Identity Theft, defined as the fraudulent acquisition and/or use of a person's private identifying information;
 - j. Spying;
 - k. Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes, except as authorized by a Department Head for the purpose of County business.
 - l. Downloading, storing, or distributing copyrighted material without proper licensing.

EMAIL USE GUIDELINES

- A. County employees shall identify themselves accurately and completely when corresponding with others by means of telephone, e-mail, Intranet, or Internet and shall not send any unsolicited mass e-mails or e-mails used for solicitation purposes with the exception of department approved emails.
- B. Email accounts will be set up for each employee determined to have a business need to send and receive County email.
- C. Employees must use the County email system for all County business-related emails. Employees are prohibited from sending County business emails from a non-County provided email account.
- D. Retrieval, interception, or reading of an email or other electronic messages not addressed to the employee, unless expressly authorized by the Department Head or by the message's original recipient, is prohibited.
- E. Limited personal usage of the County email systems is permitted at the discretion of the Department Head as long as such usage does not negatively impact the County computer network and/or such usage does not negatively impact the employee's job performance. Conducting non-County related business from a County email account is prohibited. No County data shall be sent using personal or non-County provided email.
- F. The County email systems may not be used for the following, which may include but is not limited to spamming, harassment, issuing threats, solicitations, chain letters, or pyramid schemes.
- G. The County makes the distinction between the sending of mass emails and the sending of unsolicited emails (SPAM). Mass emails may be useful and are allowed as the situation dictates with the approval of the Department Head or the Information Technology Department. Sending of SPAM emails is strictly prohibited. Mass emails must have the following characteristics. Emails sent to County employees or persons who have already inquired about the County's services are exempt from the below requirements:
 - a. The email must contain instructions on how to unsubscribe from receiving future emails. Unsubscribe requests must be honored immediately;
 - b. The email must contain a subject line relevant to the content;
 - c. The email must contain contact information, including the physical address of the sender;
 - d. The email must not contain intentionally misleading information. This excludes emails generated by the Information Technology Department for the purposes of security training.
- H. Employees are prohibited from forging email header information or attempting to impersonate another person using the County email system.
- I. Information that is considered confidential, Personally Identifiable Information (PII), or Health Insurance Portability and Accountability Act (HIPAA) information may not be sent via email to an external recipient without proper encryption applied.
- J. Suspicious emails or attachments should be forwarded to the Information

Technology Department for review.

- K.** The County requires the use of an Out of Office message if the employee will be out of the office for the entire business day or more. The message should notify the sender that the employee is out of the office, and who the sender should contact if immediate assistance is required.
- L.** Employees should be advised that the County owns and maintains all legal rights to its email system and network, and thus any email passing through these systems is owned by the County. Email may be backed up, copied, retained, or used for legal, disciplinary, or other reasons. Additionally, emails sent to or from the County may be considered public record and, therefore, subject to the Freedom of Information Act.
- M.** Accessing the County's email system from a non-County device without the permission of an employee's supervisor is prohibited.
- N.** Emails that are or may be constituted as "Records" per the State of Illinois Records Retention Act must be retained as per the regulations in that Act. Each Department's Application for Authority determines what constitutes a Record to dispose of local records. These records should be retained outside of the email system.
- O.** Employees are strictly prohibited from deleting an email in an attempt to hide a violation of this or another County policy, or where the deleted email is a "record" as defined by the Illinois Record Retention Act. Email must not be deleted when there is an active investigation or litigation where that email may be relevant.

CELLPHONE AND WIRELESS DEVICE USE GUIDELINES

The County will provide cellphones to employees where an employee is required, in the sole discretion of the Department Head, to have a cellphone to conduct County business. Exceptions will be made on a case-by-case basis and only if a special accommodation is needed. The following guidelines apply to all devices used to access the County's e-mail system.

- A.** Employees shall not download and/or save sensitive, confidential, or inappropriate information to their wireless devices unless the devices are encrypted with County approved encryption software and/or are password protected.
- B.** Employees are responsible for locking and securing their wireless devices when not in use. Please contact the Information Technology Department for procedures regarding securing wireless devices.
- C.** Purchases from the app store without prior authorization of the department head is prohibited.
- D.** Lost phones must be reported immediately to the Department Head, the Security Department, and the Information Technology Department.

SECURITY AWARENESS

Technology and information resource users are required to complete the mandatory security training and are requested to review any additional material when made available. At a minimum, this will occur annually per Illinois State Law (20 ILCS 1375/5-30) Illinois Information Security Improvement Act.

REPORTING OF A SECURITY INCIDENT

If a security incident or breach of any security policies is discovered or suspected, the employee must immediately notify his or her Department Head and the Information Technology Department. Employees must treat a suspected security incident as confidential information. Employees must not withhold information relating to a security incident or interfere with an investigation. Incidents which require notification can include:

- A.** Suspected compromise of login credentials (username, password, etc.);
- B.** Suspected virus/malware/Trojan infection;
- C.** Loss or theft of any device that contains County information;
- D.** Loss or theft of ID badge or keycard;
- E.** Any attempt by any person to obtain the user's password over the telephone or by email;
- F.** Any other suspicious event that may impact the County's information security.

POLICY VIOLATIONS

Consistent with the County's policy regarding all County workplace procedures, the following conduct is strictly prohibited in relation to Technology Resources:

- A.** Engaging in fraud, misrepresentation, or providing false information to the County.
- B.** Failure to comply with employees' obligations under this policy to include Network Guidelines, Computer Use Guidelines, Email Use Guidelines, and Cellphone and Wireless Device Use Guidelines.
- C.** Knowingly using County-owned or County-provided computer systems or equipment for activities that are considered illegal under local, state, federal, or international law.

Employees who engage in such conduct will be subject to discipline, up to and including discharge.



Policy 8.1	Technology Resources Acceptable Use		
<u>Effective Date:</u> 2/28/12 <u>Last Amended Date:</u> 4/8/2025	<u>Applicable Law/Statute:</u> None Illinois Information Security Improvement Act (20 ILCS 1375/5-30) Personal Information Protection Act (815 ILCS 530)	<u>Source Doc/Dept.:</u> None/IT	<u>Authorizing I.C. Sec.:</u> None

TECHNOLOGY RESOURCES ACCEPTABLE USE

8.1

POLICY

It is the policy of DuPage County's policy is to provides employees with technology resources that are necessary to support our goals and objectives. This policy pertains to all technology-related equipment, hardware, and software, including, but not limited to County-owned, leased, or licensed desktop and laptop computers, tablets, telephones, cell phones, copy machines, fax machines, computer systems, e-mail, other messaging software, Intranet, and Internet services, tools, and supplies.

ELIGIBILITY

- All employees under County Board jurisdiction, regardless of employment status. To the extent that this policy constitutes a term or condition of employment which is required to be bargained under any collective bargaining agreement, employees covered by such an agreement shall not be subject to the terms of this policy until such time as the bargaining agreement is amended or the policy terms are agreed to by the unit.

GUIDELINES

- A. The use of County technology resources are is intended primarily for County business use; however, incidental and occasional use of these systems for non-work purposes that does not result in a negative budgetary or performance impact may be permitted at the discretion of the Department Head under the following conditions:
 - a. Must not result in direct costs, cause legal action against, or negatively impact the County.
 - b. Must not interfere with the performance of work duties.
 - c. Must not cause a noticeable impact or change to operational infrastructure systems, noticeably consume resources, incur support, or otherwise adversely affect the functioning of essential operations.

- d. DuPage County reserves the right to monitor personal use to ensure compliance with all policies and determine whether it is considered "Incidental Use" at the County's sole discretion.
- B. County employees shall have no expectation of privacy ~~in terms of~~ regarding their use of County technology resources. The County reserves the right to access any and all information, including files and e-mail, stored on the County network or any County equipment. ~~The County may at any time examine technology or information resources, or intercept, monitor, review, and share data with authorized personnel and law enforcement if necessary.~~
- C. All County employees ~~are expected to conduct themselves honestly and appropriately~~ must use County technology resources in a manner that complies with applicable laws and policies. ~~In doing so, employees are expected to respect~~ This includes adhering to the Freedom of Information Act, copyrights and software licensing rules, property rights, and the privacy of others protections. ~~The County's computer system must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Examples of this include:~~
 - a. Copying and sharing images, music, movies, or other copyrighted material using P2P (peer to peer) file sharing, or unlicensed CD's and DVD's;
 - b. Posting or plagiarizing copyrighted material;
 - c. Downloading copyrighted files which the employee has not already legally procured;
 - d. Software without a valid license or from an unapproved source
- D. Employees are expected to exercise good judgment regarding appropriate use of County technology resources and equipment, and adhere to any safety guidelines related to a piece of equipment.
- ~~E. County employees shall identify themselves accurately and completely when corresponding with others by means of telephone, e-mail, Intranet or Internet and shall not send any unsolicited mass e-mails or e-mails used for solicitation purposes with the exception of County supported charities. At no time may County e-mail be used in a manner which gives the impression that the County has authorized an otherwise personal communication.~~
- E. Employees are expected to limit the use of personal phones, pagers, PDA devices, MP3 players, electronic devices and other personal equipment for non-work-related purposes during working hours. Any limited use will be at the discretion of the Department Head.
- F. Employees may not blog, or use other forms of commonly known social media or technology ~~on~~ **using County equipment on** the Internet/intranet during their designated work schedule, unless specifically authorized by the Department Head as part of the

employee's position. ~~Blogging or other forms of social media or technology include, but are not limited to, social networks, online dating, video, wiki postings, personal blogs, or other similar forms of online journals, diaries, and personal newsletters not affiliated with DuPage County.~~

~~G. DuPage County reserves the right to monitor employee use of County equipment, blogs, and other social media. Employees shall have no expectation of privacy with regard to the use of any County equipment or content that they post. In addition, DuPage County reserves the right to discontinue employee access to equipment~~ County equipment, require employees to remove or stop posting content if an employee is found to have posted content that is deemed inappropriate including, but not limited to, content which:

1. Violates any laws
2. Is libelous or may be construed as harassment. (Personnel Policy 7.4: Harassment)
3. Violates any County policies, rules, standards or requirements including, but not limited to, the County's Ethics Ordinance and Personnel Policy 9.1: Employment Ethics
4. Is adverse to the reputation, interests or business relationships of DuPage County

H. Instant messaging such as Microsoft Teams is allowed for County businesses communications only.

~~I. Employees may not take County Equipment home, unless otherwise authorized by the Department Head.~~ **Employees may not remove County equipment from the location where the equipment is assigned, except for cellular devices, equipment installed in vehicles, or equipment intended to be used in the field unless otherwise authorized by the Department Head and Information Technology. Once approved, Information Technology must be notified in order to update their records. Upon separation, all technology resources must be returned to the Information Technology Department..**

~~J. County employees~~ Employees shall not install, remove, or otherwise modify any hardware or software without written approval of their Department Head and ~~IT Department~~ Information Technology.

K. Employees will be issued one desktop or laptop for their use. Employees will not be allowed multiple desktops or laptops for their sole use unless authorized by their Department Head and Information Technology. Kiosks or computers for use by multiple employees are exempt from this requirement.

L. Employees are responsible for ensuring the protection and security of assigned County technology resources. Technology resources must be secured when not in use. Missing

equipment must be reported to the Department Head, ~~Security Office~~ Security Department, and ~~the IT Department~~ Information Technology immediately.

- a. Laptop locks and cables must be used to secure laptops when in a non-secured area;
- b. Mobile devices must be kept out of sight when not in use;
- c. Care must be given when using or transporting devices in busy areas;
- d. Generally, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.

NETWORK USE GUIDELINES

- A. The DuPage County Information Technology ~~department~~ Department shall be the sole provider of designs, specifications, operations, maintenance, and management of all network infrastructure and equipment including, but not limited to, ~~wireless access points~~ switches, routers, firewalls, wireless access points, and the wired/wireless local area network, **except for departments that have their own network staff.**
- B. With the exception of the ~~IT Department~~ Information Technology Department, and other employees approved by their Department Head and the ~~CIO~~ Chief Information Officer (CIO), no ~~E~~employee shall be granted administrative rights to any ~~N~~network equipment.
- C. Remote access to the County systems shall only be allowed via County approved software and hardware. **Remote access systems are to be used in the same manner as computer systems within the County offices and are subject to the same policies. Employees shall ensure reasonable physical security is maintained for the computing systems used for remote access.**
- D. Non-County provided equipment is expressly prohibited on the County's network.**

COMPUTER USE GUIDELINES

- A. Employees ~~will~~ must safeguard login ~~identifications~~ identifiers and passwords. Any suspected password compromise ~~will~~ must be reported immediately to the ~~IT Department~~ Information Technology Department. Password and access information may not be recorded, shared, or given to anyone other than the ~~E~~employee
- B. **No employee shall allow non-County Information Technology staff to assume unsupervised control of a computer or application to which you have logged in with your username.**
- C. ~~All Employees are responsible for logging out of or locking their workstation before they leave the office/desk unattended so that unauthorized persons cannot see, read or take/copy confidential data. Contact the IT Department for procedures concerning automatic locking of workstations.~~ **All employees are responsible for locking or logging**

out of their workstation before they leave the office/desk unattended.

- D. ~~With the exception of the IT Department, and other employees approved by their Department Head and the CIO, no Employees shall be granted administrative rights to their workstation.~~ No employee shall be granted a primary login with administrative rights to their workstation, except as approved by their Department Head or the Chief Information Officer.
- E. ~~No personal data shall be stored on County Servers. This includes, but is not limited to, documents, pictures, music and video files.~~ No personal data shall be stored on County servers. This includes but is not limited to, documents, pictures, music, and video files. The Information Technology Department reserves the right to remove any personal documents, pictures, music, or video files without warning. Findings shall be reported to the employee's supervisor.
- F. ~~No confidential data shall be stored on any local or removable media devices that are not encrypted with County approved encryption software.~~ No confidential information shall be stored on any local or removable media devices that are not encrypted with County approved encryption software
- G. ~~Data stored locally on desktops and laptops is not backed up by the IT Department. No County business related data shall be stored on any local hard drives. The IT Department will provide training to ensure that data is being stored in the correct location.~~ No County business-related data shall be stored on any local hard drives. The Information Technology Department will provide training to ensure that data is being stored in the correct location.
- H. No County data shall be shared using non-County provided storage unless required by an outside vendor and with the approval of the Department Head.
- I. ~~Employees are prohibited from making modifications to County-owned technology without appropriate approval from their Department Head and the IT Department. Modifications that could impact the County network, desktop computing devices and other computer systems are strictly prohibited. Modification includes, but is not limited to, software installation and configuration changes. Installation of non-business related software, personal music and video files is prohibited.~~ Employees are prohibited from modifying County-owned technology without approval from their Department Head and Information Technology Department. These modifications include, but are not limited to, software installation, hardware installation, and configuration changes. Installation of non-business-related software is prohibited.
- J. While the County permits limited personal Internet usage, the County assumes no responsibility for any content that the employee may view or read that they find offensive. The County may use software to filter offensive, sexually explicit, inappropriate, or non-business-related sites.

- K.** Streaming media, such as internet radio stations or internet videos, is allowed for job-related functions only, subject to the approval of the Department Head and/or Information Technology Department.
- L.** Excessive use, as defined by the Information Technology Department, of County bandwidth or other computer resources is not permitted. Bandwidth-intensive tasks that may degrade network capacity or performance such as large file downloads or uploads or streaming audio or video should be coordinated with the Information Technology Department. If contacted by the Information Technology Department with regards to the excessive use of bandwidth employees will follow the instructions of the Information Technology Department.
- M.** Utilizing county-owned or county-provided computer systems to bypass any established security, authentication, or user-access controls is strictly prohibited. Any deliberate attempt to circumvent these security measures, including efforts to escalate privileges, is expressly forbidden
- N.** ~~The following examples are unacceptable uses of County technology equipment: downloading non-work related files, including music files; personal instant messaging or chat; playing games; sending chain letters; sending, printing or displaying offensive images, pictures or jokes; sending, printing or displaying sexually offensive materials; sending, initiating or contributing to "SPAM"; running "Hacker" or "Cracker" type software or actions; using proxy sites or servers; using Peer to Peer or file sharing software; FTP software; streaming audio and video for any purpose unless authorized and configured by the IT Department to support a valid County business requirement; causing damage to County owned computers and/or peripheral equipment. Said list is of examples is not meant to represent all unacceptable uses of County technology.~~ **Illegal activities using County-owned or County-provided computer systems are prohibited. Such actions include but are not limited to:**
- a)** Unauthorized port scanning, defined as systematically scanning a computer's ports;
 - b)** Unauthorized network hacking, defined as any technical effort to manipulate the normal behavior of network connections and connected systems;
 - c)** Unauthorized packet sniffing, defined as the act of capturing packets of data flowing across a computer network;
 - d)** Unauthorized packet spoofing, defined as creating internet protocol packets with a false source IP address;
 - e)** Unauthorized Denial of Services, defined as a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users;
 - f)** Unauthorized wireless hacking, defined as accessing wireless networks by defeating the security devices within that wireless network;
 - g)** Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system;
 - h)** Acts of Terrorism;
 - i)** Identity Theft, defined as the fraudulent acquisition and/or use of a person's private identifying information;

- j) Spying;
- k) Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes, except as authorized by a Department Head for the purpose of County business.
- l) Downloading, storing, or distributing copyrighted material without proper licensing

EMAIL USE GUIDELINES

- A. County employees shall identify themselves accurately and completely when corresponding with others by means of telephone, e-mail, Intranet, or Internet and shall not send any unsolicited mass e-mails or e-mails used for solicitation purposes with the exception of ~~County-supported charities~~ **department approved emails**. ~~At no time may County e-mail be used in a manner which gives the impression that the County has authorized an otherwise personal communication.~~
- B. Email accounts will be set up for each employee determined to have a business need to send and receive County email.
- C. Employees must use the County email system for all County business-related emails. Employees are prohibited from sending County business emails from a non-County provided email account.
- D. Retrieval, interception, or reading of an email or other electronic messages not addressed to the employee, unless expressly authorized by the Department Head or by the message's original recipient, is prohibited.
- E. Limited personal usage of the County email systems is permitted at the discretion of the Department Head as long as such usage does not negatively impact the County computer network and/or such usage does not negatively impact the employee's job performance. Conducting non-County related business from a County email account is prohibited. No County data shall be sent using personal or non-County provided email.
- F. The County email systems may not be used for the following, which may include but is not limited to spamming, harassment, issuing threats, solicitations, chain letters, or pyramid schemes.
- G. The County makes the distinction between the sending of mass emails and the sending of unsolicited emails (SPAM). Mass emails may be useful and are allowed as the situation dictates with the approval of the Department Head or the Information Technology Department. Sending of SPAM emails is strictly prohibited. Mass emails must have the following characteristics. Emails sent to County employees or persons who have already inquired about the County's services are exempt from the below requirements:
 - a. The email must contain instructions on how to unsubscribe from receiving future emails. Unsubscribe requests must be honored immediately;
 - b. The email must contain a subject line relevant to the content;
 - c. The email must contain contact information, including the physical address of the sender;
 - d. The email must not contain intentionally misleading information. This excludes emails generated by the Information Technology Department for the purposes of security training.
- H. Employees are prohibited from forging email header information or attempting to impersonate another person using the County email system.

- I. Information that is considered confidential, Personally Identifiable Information (PII), or Health Insurance Portability and Accountability Act (HIPAA) information may not be sent via email to an external recipient without proper encryption applied.
- J. Suspicious emails or attachments should be forwarded to the Information Technology Department for review.
- K. The County requires the use of an Out of Office message if the employee will be out of the office for the entire business day or more. The message should notify the sender that the employee is out of the office, and who the sender should contact if immediate assistance is required.
- L. Employees should be advised that the County owns and maintains all legal rights to its email system and network, and thus any email passing through these systems is owned by the County. Email may be backed up, copied, retained, or used for legal, disciplinary, or other reasons. Additionally, emails sent to or from the County may be considered public record and, therefore, subject to the Freedom of Information Act.
- M. Accessing the County's email system from a non-County device without the permission of an employee's supervisor is prohibited.
- N. Emails that are or may be constituted as "Records" per the State of Illinois Records Retention Act must be retained as per the regulations in that Act. Each Department's Application for Authority determines what constitutes a Record to dispose of local records. These records should be retained outside of the email system.
- O. Employees are strictly prohibited from deleting an email in an attempt to hide a violation of this or another County policy, or where the deleted email is a "record" as defined by the Illinois Record Retention Act. Email must not be deleted when there is an active investigation or litigation where that email may be relevant.

CELLPHONE AND WIRELESS DEVICE USE GUIDELINES

The County will provide cellphones to employees where an employee is required, in the sole discretion of the Department Head, to have a cellphone to conduct County business. Exceptions will be made on a case-by-case basis and only if a special accommodation is needed. The following guidelines apply to ~~any and all~~ devices used to access the County's e-mail system.

- A. Employees shall not download and/or save sensitive, confidential, or inappropriate information to their wireless devices unless the devices are encrypted with County approved encryption software, and/or ~~password protected~~ **are password protected**.
- B. Employees are responsible for locking and securing their wireless devices ~~–Please contact the IT Department for procedures regarding securing wireless devices.~~ **when not in use. Please contact the Information Technology Department for procedures regarding securing wireless devices.**
- C. ~~All wireless devices that access the County's e-mail system must have the ability to be disabled remotely.~~
 - D. ~~Installation of non-business related applications or software that results in any cost to the County is prohibited.~~ **Purchases from the app store without prior authorization of the department head is prohibited.**

- ~~D. Lost phones must be reported immediately to the Department Head, Security Office and the IT Department.~~ Lost phones must be reported immediately to the Department Head, the Security Department, and the Information Technology Department.

SECURITY AWARENESS

Technology and information resource users are required to complete the mandatory security training and are requested to review any additional material when made available. At a minimum, this will occur annually per Illinois State Law (20 ILCS 1375/5-30) Illinois Information Security Improvement Act.

REPORTING OF A SECURITY INCIDENT

If a security incident or breach of any security policies is discovered or suspected, the employee must immediately notify his or her Department Head and the Information Technology Department. Employees must treat a suspected security incident as confidential information. Employees must not withhold information relating to a security incident or interfere with an investigation. Incidents which require notification can include:

- A.** Suspected compromise of login credentials (username, password, etc.);
- B.** Suspected virus/malware/Trojan infection;
- C.** Loss or theft of any device that contains County information;
- D.** Loss or theft of ID badge or keycard;
- E.** Any attempt by any person to obtain the user's password over the telephone or by email;
- F.** Any other suspicious event that may impact the County's information security.

POLICY VIOLATIONS

Consistent with the County's policy regarding all County workplace procedures, the following conduct is strictly prohibited in relation to Technology Resources:

- A.** Engaging in fraud, misrepresentation, or providing false information to the County.
- B.** Failure to comply with employees' obligations under this policy to include Network Guidelines, Computer Use Guidelines, Email Use Guidelines, and Cellphone and Wireless Device Use Guidelines.
- C.** Knowingly using County-owned or County-provided computer systems or equipment for activities that are considered illegal under local, state, federal, or international law.

~~Inappropriate use of County-owned equipment may result in disciplinary action, not to exclude termination. (Personnel Policy 10.1: Disciplinary Guidelines)~~

Employees who engage in such conduct will be subject to discipline, up to and including discharge.



Technology **Acceptable Use Policy (AUP)** Resolution

What is the DP Technology Resource Acceptable Use Policy?

DuPage County’s Technology Resource Acceptable Use Policy (AUP) outlines the rules governing the use of DuPage County’s technology, including computers, internet access, email, and software. It helps make sure everyone uses these tools safely, responsibly, and legally.

Benefits of an AUP include:

- Protects DuPage County from security risks and legal issues
- Sets clear expectations for behavior while using technology
- Helps prevent misuse of technology
- Promotes a safe and productive digital environment

What are you requesting?

Approval to revise the Technology Resources Acceptable Use Policy. The current AUP was last updated in 2016.





Technology **Acceptable Use Policy (AUP)** Resolution

What's changing?

- Removed out-of-scope targets from the policy. (i.e., volunteers)
- Added collective bargaining agreement language
- Updated/modernized technical language throughout
- Replaced suggestive language with direct language (e.g., employees should vs will)
- New requirement for reporting security incidents





Technology Change Order with Resolution

421 N. COUNTY FARM
ROAD
WHEATON, IL 60187
www.dupagecounty.gov

File #: TE-CO-0003-25

Agenda Date: 4/1/2025

Agenda #: 7.A.

AMENDMENT TO COUNTY CONTRACT 6082-0001 SERV
ISSUED TO DELL, INC.
FOR MICROSOFT ENTERPRISE AGREEMENT
FOR INFORMATION TECHNOLOGY
(INCREASE ENCUMBRANCE \$7,470.00, 0.19%)

WHEREAS, County Contract 6082-0001 SERV was approved by the Technology Committee on November 1, 2022; and

WHEREAS, the Technology Committee recommends changes as stated in the Change Order Notice to County Contract 6082-0001 SERV, issued to Dell, Inc., for Microsoft Enterprise Agreement (EA) for all Microsoft Software and Azure Cloud Services, for GIS and Information Technology, to increase the contract by \$7,470.00, resulting in an amended contract total of \$3,857,514.05, an increase of 0.19%.

NOW, THEREFORE BE IT RESOLVED, that the County Board adopt the Change Order Notice to County Contract 6082-0001 SERV, issued to Dell, Inc., for Microsoft Enterprise Agreement (EA) for all Microsoft Software and Azure Cloud Services, for GIS and Information Technology, to increase the contract by \$7,470.00 resulting in an amended contract total of \$3,857,514.05, an increase of 0.19%.

Enacted and approved this 8th day of April, 2025 at Wheaton, Illinois.

DEBORAH A. CONROY, CHAIR
DU PAGE COUNTY BOARD

Attest: _____

JEAN KACZMAREK, COUNTY CLERK

TEC 4/1
 FI/CB 4/8



Request for Change Order
Procurement Services Division

Attach copies of all prior Change Orders

Date: Mar 14, 2025

MinuteTraq (IQM2) ID #: _____

Purchase Order #: 6082-1-SERV	Original Purchase Order Date: Dec 1, 2022	Change Order #: 5	Department: IT
Vendor Name: Dell Inc.	Vendor #: 10850		Dept Contact: Joe Hamlin
Background and/or Reason for Change Order Request:	Add a new line for 30 M365 Co-Pilot licenses in the amount of \$7,470.00 against 1000-1110-53807. This is a new license Microsoft recently released and was not available when this agreement was renewed.		
IN ACCORDANCE WITH 720 ILCS 5/33E-9			

- (A) Were not reasonably foreseeable at the time the contract was signed.
- (B) The change is germane to the original contract as signed.
- (C) Is in the best interest for the County of DuPage and authorized by law.

INCREASE/DECREASE	
A	Starting contract value \$3,838,349.52
B	Net \$ change for previous Change Orders \$11,694.53
C	Current contract amount (A + B) \$3,850,044.05
D	Amount of this Change Order <input checked="" type="checkbox"/> Increase <input type="checkbox"/> Decrease \$7,470.00
E	New contract amount (C + D) \$3,857,514.05
F	Percent of current contract value this Change Order represents (D / C) 0.19%
G	Cumulative percent of all Change Orders (B+D/A); (60% maximum on construction contracts) 0.50%

DECISION MEMO NOT REQUIRED

Cancel entire order
 Close Contract
 Contract Extension (29 days)
 Consent Only

Change budget code from: _____ to: _____

Increase/Decrease quantity from: _____ to: _____

Price shows: _____ should be: _____

Decrease remaining encumbrance and close contract
 Increase encumbrance and close contract
 Decrease encumbrance
 Increase encumbrance

DECISION MEMO REQUIRED

Increase (greater than 29 days) contract expiration from: _____ to: _____

Increase ≥ \$2,500.00, or ≥ 10%, of current contract amount
 Funding Source _____

OTHER - explain below: _____

SJG	5037	Mar 14, 2025	<u>RAB</u>	5064	03/17/2025
Prepared By (Initials)	Phone Ext	Date	Recommended for Approval (Initials)	Phone Ext	Date
REVIEWED BY (Initials Only)					
Buyer	Date			Procurement Officer	Date
				3/19/2025	
Chief Financial Officer (Decision Memos Over \$25,000)	Date	Chairman's Office (Decision Memos Over \$25,000)	Date		



Decision Memo

Procurement Services Division

This form is required for all Professional Service Contracts over \$25,000 and as otherwise required by the Procurement Review Checklist.

Date: Mar 14, 2025

File ID #: _____

Purchase Order #: 6082-1-SERV

Requesting Department: IT	Department Contact: Joe Hamlin
Contact Email: Joe.Hamlin@dupagecounty.gov	Contact Phone: x5063
Vendor Name: Dell Inc.	Vendor #: 10850

Action Requested - Identify the action to be taken and the total cost; for instance, approval of new contract, renew contract, increase contract, etc.

Add a new line for 30 M365 Co-Pilot licenses in the amount of \$7,470.00 against 1000-1110-53807.

Summary Explanation/Background - Provide an executive summary of the action. Explain why it is necessary and what is to be accomplished.

Microsoft recently released this software for government customers. These licenses will be used to pilot use cases with the county's Information Technology department and the county-wide AI Committee. Microsoft recently released this software for government customers

Original Source Selection/Vetting Information - Describe method used to select source.

NASPO SVAR - Illinois PA Contract #C000001197009

Recommendations/Alternatives - Describe staff recommendation and provide justification. Identify at least 2 other options to accomplish this request.

None - Microsoft CoPilot is the only AI platform integrated with M365/Office and Windows.

Fiscal Impact/Cost Summary - Include projected cost for each fiscal year, approved budget amount and account number, source of funds, and any future funding requirements along with any narrative.

\$7,470.00 - FY2025 - 1000-1110-53807



A quote for your consideration

Based on your business needs, we put the following quote together to help with your purchase decision. Below is a detailed summary of the quote we've created to help you with your purchase decision.

To proceed with this quote, you may respond to this email, order online through your [Premier page](#).

Quote No.	3000186576021.1	Sales Rep	Christian Reed
Total	\$7,470.00	Phone	1(800) 456-3355, +17375876700
Customer #	530032141573	Email	Christian_Reed@Dell.com
Quoted On	Mar. 04, 2025	Billing To	ACCOUNTS PAYABLE
Expires by	Mar. 31, 2025		COUNTY OF DUPAGE
Contract Name	NASPO SVAR - Illinois PA		421 N COUNTY FARM RD
Contract Code	C000001197009		WHEATON, IL 60187-2553
Customer Agreement #	CTR060024		

Message from your Sales Rep

Please use the Order button to securely place the order with your preferred payment method online. You may contact your Dell sales team if you have any questions. Thank you for shopping with Dell.

Regards,
Christian Reed


Shipping Group

Shipping To	Shipping Method
ACCOUNTS RECEIVABLE COUNTY OF DUPAGE 421 N COUNTY FARM RD WHEATON, IL 60187-2553 (630) 407-5053	Standard Delivery

	Quantity	Unit Price	Subtotal
8020472			
1. VLA ENTERPRISE M365 COPILOT GCC SUB ADD-ON	30	\$249.00	\$7,470.00

Subtotal:	\$7,470.00
Shipping:	\$0.00
Non-Taxable Amount:	\$7,470.00
Taxable Amount:	\$0.00
Estimated Tax:	\$0.00

Total:	\$7,470.00
--------	------------



Accelerate the power
of AI for your data

Take the first step in achieving
Generative AI success

[Learn More](#)

Shipping Group Details

Shipping To

ACCOUNTS RECEIVABLE
COUNTY OF DUPAGE
421 N COUNTY FARM RD
WHEATON, IL 60187-2553
(630) 407-5053

Shipping Method

Standard Delivery

	Quantity	Unit Price	Subtotal
8020472			
1. VLA ENTERPRISE M365 COPILOT GCC SUB ADD-ON	30	\$249.00	\$7,470.00
SKU: AD284467	MFG Part #: EP2-24658	OLS Purchase Type:	
Current Duration:	Total Duration:	Maint. End Date: Nov. 30, 2025	

Important Notes

Terms of Sale

This Quote will, if Customer issues a purchase order for the quoted items that is accepted by Supplier, constitute a contract between the entity issuing this Quote ("Supplier") and the entity to whom this Quote was issued ("Customer"). Unless otherwise stated herein, pricing is valid for thirty days from the date of this Quote. All product, pricing and other information is based on the latest information available and is subject to change. Supplier reserves the right to cancel this Quote and Customer purchase orders arising from pricing errors. Taxes and/or freight charges listed on this Quote are only estimates. The final amounts shall be stated on the relevant invoice. Additional freight charges will be applied if Customer requests expedited shipping. Please indicate any tax exemption status on your purchase order and send your tax exemption certificate to Tax_Department@dell.com or ARSalesTax@emc.com, as applicable.

Governing Terms: This Quote is subject to: (a) a separate written agreement between Customer or Customer's affiliate and Supplier or a Supplier's affiliate to the extent that it expressly applies to the products and/or services in this Quote or, to the extent there is no such agreement, to the applicable set of Dell's Terms of Sale (available at www.dell.com/terms or www.dell.com/oemterms), or for cloud/as-a-Service offerings, the applicable cloud terms of service (identified on the Offer Specific Terms referenced below); and (b) the terms referenced herein (collectively, the "Governing Terms"). Different Governing Terms may apply to different products and services on this Quote. The Governing Terms apply to the exclusion of all terms and conditions incorporated in or referred to in any documentation submitted by Customer to Supplier.

Supplier Software Licenses and Services Descriptions: Customer's use of any Supplier software is subject to the license terms accompanying the software, or in the absence of accompanying terms, the applicable terms posted on www.Dell.com/eula. Descriptions and terms for Supplier-branded standard services are stated at www.dell.com/servicecontracts/global or for certain infrastructure products at www.dellemc.com/en-us/customer-services/product-warranty-and-service-descriptions.htm.

Offer-Specific, Third Party and Program Specific Terms: Customer's use of third-party software is subject to the license terms that accompany the software. Certain Supplier-branded and third-party products and services listed on this Quote are subject to additional, specific terms stated on www.dell.com/offeringsspecificterms ("Offer Specific Terms").

In case of Resale only: Should Customer procure any products or services for resale, whether on standalone basis or as part of a solution, Customer shall include the applicable software license terms, services terms, and/or offer-specific terms in a written agreement with the end-user and provide written evidence of doing so upon receipt of request from Supplier.

In case of Financing only: If Customer intends to enter into a financing arrangement ("Financing Agreement") for the products and/or services on this Quote with Dell Financial Services LLC or other funding source pre-approved by Supplier ("FS"), Customer may issue its purchase order to Supplier or to FS. If issued to FS, Supplier will fulfill and invoice FS upon confirmation that: (a) FS intends to enter into a Financing Agreement with Customer for this order; and (b) FS agrees to procure these items from Supplier. Notwithstanding the Financing Agreement, Customer's use (and Customer's resale of and the end-user's use) of these items in the order is subject to the applicable governing agreement between Customer and Supplier, except that title shall transfer from Supplier to FS instead of to Customer. If FS notifies Supplier after shipment that Customer is no longer pursuing a Financing Agreement for these items, or if Customer fails to enter into such Financing Agreement within 120 days after shipment by Supplier, Customer shall promptly pay the Supplier invoice amounts directly to Supplier.

Customer represents that this transaction does not involve: (a) use of U.S. Government funds; (b) use by or resale to the U.S. Government; or (c) maintenance and support of the product(s) listed in this document within classified spaces. Customer further represents that this transaction does not require Supplier's compliance with any statute, regulation or information technology standard applicable to a U.S. Government procurement.

For certain products shipped to end users in California, a State Environmental Fee will be applied to Customer's invoice. Supplier encourages customers to dispose of electronic equipment properly.

Electronically linked terms and descriptions are available in hard copy upon request.



Required Vendor Ethics Disclosure Statement

Failure to complete and return this form may result in delay or cancellation of the County's Contractual Obligation.

Date: 3.20.2025

Bid/Contract/PO #: _____

Company Name: Dell Marketing L.P.	Company Contact: Phillip Reavis
Contact Phone: 1800-289-3355	Contact Email: phillip.reavis@dell.com

The DuPage County Procurement Ordinance requires the following written disclosures prior to award:

1. Every contractor, union, or vendor that is seeking or has previously obtained a contract, change orders to one (1) or more contracts, or two (2) or more individual contracts with the county, shall provide to Procurement Services Division a written disclosure of all political campaign contributions made by such contractor, union, or vendor within the current and previous calendar year to any incumbent county board member, county board chairman, or countywide elected official whose office the contract to be awarded will benefit. The contractor, union or vendor shall update such disclosure annually during the term of a multi-year contract and prior to any change order or renewal requiring approval by the county board. For purposes of this disclosure requirement, "contractor or vendor" includes owners, officers, managers, lobbyists, agents, consultants, bond counsel and underwriters counsel, subcontractors and corporate entities under the control of the contracting person, and political action committees to which the contracting person has made contributions.

NONE (check here) - If no contributions have been made

Add Line	Recipient	Donor	Description (e.g. cash, type of item, in-kind services, etc.)	Amount/Value	Date Made
x					

2. All contractors and vendors who have obtained or are seeking contracts with the county shall disclose the names and contact information of their lobbyists, agents and representatives and all individuals who are or will be having contact with county officers or employees in relation to the contractor bid and shall update such disclosure with any changes that may occur.

NONE (check here) - If no contacts have been made

Add Line	Lobbyists, Agents and Representatives and all individuals who are or will be having contact with county officers or employees in relation to the contract or bid	Telephone	Email
x			

A contractor or vendor that knowingly violates these disclosure requirements is subject to penalties which may include, but are not limited to, the immediate cancellation of the contract and possible disbarment from future county contracts.

Continuing disclosure is required, and I agree to update this disclosure form as follows:

- If information changes, within five (5) days of change, or prior to county action, whichever is sooner
- 30 days prior to the optional renewal of any contract
- Annual disclosure for multi-year contracts on the anniversary of said contract
- With any request for change order except those issued by the county for administrative adjustments

The full text for the county's ethics and procurement policies and ordinances are available at:

http://www.dupagecounty.gov/government/county_board/ethics_at_the_county/

I hereby acknowledge that I have received, have read, and understand these requirements.

Authorized Signature Signature on File

Printed Name Heidell Del Rio

Title Analyst, Proposal Management

Date 3.20.2025

Attach additional sheets if necessary. Sign each sheet and number each page. Page _____ of _____ (total number of pages)



Authorization to Travel

421 N. COUNTY FARM
ROAD
WHEATON, IL 60187
www.dupagecounty.gov

File #: 25-0812

Agenda Date: 4/1/2025

Agenda #: 8.A.



DuPage County Employee Overnight Business Travel Expense Reimbursement

Request

This expense form is used to request advance approval for County reimbursement of **overnight travel expenses**. Advance approval is required for County reimbursement for all overnight travel whether in-state or out-of-state. After travel is completed, a separate [Overnight Business Travel Report Form](#) must be completed and submitted to receive reimbursement for travel expenses.

Elected Officials subject to 50 ILCS 150/15 should not use this Overnight Business Travel Request Form. [Applicable form for Elected Officials subject to 50 ILCS 150/15.](#)

Do not use this form for travel that does not include an overnight stay. Advance approval is not required for travel that does not include an overnight stay.

Written documentation is not required for approval prior to travel. However, complete itemized documentation is required for reimbursement after travel.

Please review the [County's Business Travel Expense Policy](#) before completing this form.

The County's Business Travel Expense Policy : ["Yes"]

Employee Name: [REDACTED]

Employee Email Address: [REDACTED]

Department: IT

Supervisor Email: Viji.Ramaswamy@dupagecounty.gov

Secondary Department Contact (Department Admin or Accounts Payable):

Sarah.Godzicki@dupagecounty.gov

Description of the Requested Business Travel

Description of conference, training or other out of town event: Tyler Connect 2025 conference. It is related to the Tyler application Dupage County users and it supports for Property Taxes.

Start date of conference, training or other out of town event: 05-11-2025

End date of conference, training or other out of town event: 05-14-2025

Departure travel date: 05-11-2025

Return travel date: 05-14-2025

If travel dates extend before or after the dates related to the purpose of travel, explain why the additional travel days are necessary: N/A

Estimate of costs for the requested business travel

Budget Account Code: 1000-1110

Registration fees for conference, training or event: \$1199

Form of Payment: Invoiced to county

Estimated transportation cost to and from location: \$1000

Describe methods of transportation to and from location: Flights to and from san antonio and taxi/rideshare

to and from airport

Rental Vehicle request:

Provide estimated rental car cost: \$

Describe reason(s) for vehicle rental:

Business Travel Expense Policy - Supplemental Insurance:

Total Estimated Lodging Costs: \$790

Description of lodging needs, including number of nights and cost per night: sunday through wednesday at 263.21 per night

Meal Per Diem Policy

See **Business Travel Expense Policy Section 6.0** regarding meal per diems. Individual meals, **including room service**, are not reimbursable and meal receipts are not required or accepted. Tips are included in the per diem and are not reimbursable. Per diems are paid at 100% of applicable GSA CONUS rates for non-travel days and at 75% of applicable GSA CONUS rates for the travel day at the beginning of the trip and the travel day for returning from the trip.

See the per diem rates at <https://www.gsa.gov/travel/plan-book/per-diem-rates>.

Estimate Total Per Diem expenses: \$215

Estimate such additional expenses: \$0

Describe expected additional expenses:

Estimated total cost of the requested Overnight Business Travel: \$3204

Confirmation and Submission

By typing my name below, the employee submitting this request certifies that the information provided herein accurately describes the proposed business travel and the requested travel expenses are my best estimate of the costs and expenses related to that travel. I understand that this request requires advance approval by my Department Head and the Parent Committee Chair (if the total is not more than \$2,500) or the Parent Committee (if the total is more than \$2,500).

Employee Name: [REDACTED]

Instructions for Immediate Supervisor other than Department Head

Please review this Overnight Business Travel Request Form. If you approve the requested travel, please forward the form by email to the Department Head and indicate your approval.

Instructions for Department Head

Please review this Overnight Business Travel Request Form. If you approve the requested travel, please print this form, sign below, scan and email to the Chair of the relevant Parent Committee.

Instructions for Parent Committee Chair

Please review this Overnight Business Travel Request Form. If \$2,500 or less, and you approve the requested travel, please print this form, sign below, scan, and return via email to the Department Head. If more than \$2,500, place this item on the agenda of the relevant Parent Committee. After approval by the Parent Committee, please print this form, sign below, scan, and return via email to the Department Head.

REVIEWED BY AND DATE APPROVED:

Department Head: Signature on File

Date: 03/20/2025

Committee Chair: _____

Date: _____

If the request is over \$2,500 the Committee Chair certifies that the travel was approved by a majority vote at a scheduled meeting of the Parent Committee

Committee Name: Technology Committee

Meeting Date: 04/01/2025



Judicial/Public Safety Resolution

421 N. COUNTY FARM
ROAD
WHEATON, IL 60187
www.dupagecounty.gov

File #: JPS-R-0005-25

Agenda Date: 4/1/2025

Agenda #: 6.A.

RESOLUTION TO RESCIND JPS-P-0039-24
ISSUED TO VIDEO AND SOUND SERVICE, INC.
TO PROVIDE MAINTENANCE AND REPAIR
OF THE CAMPUS SECURITY SYSTEM, AS NEEDED,
FOR THE COUNTY CAMPUS
(CONTRACT TOTAL AMOUNT OF \$301,582)

WHEREAS, on November 26, 2024, the DuPage County Board approved JPS-P-0039-24 for a contract purchase order to Video and Sound Service, Inc., to provide maintenance and repair of the campus security system, as needed, for the County campus, for the two-year period, December 1, 2024, through November 30, 2026, for the Office of Homeland Security and Emergency Management; and

WHEREAS, the awarded vendor is unable to meet all of the qualifications on the original bid #24-105-OHSEM.

NOW, THEREFORE, BE IT RESOLVED, by the DuPage County Board that Resolution JPS-P-0039-24, dated November 26, 2024, shall be and is hereby repealed and rescinded in its entirety effective immediately.

Enacted and approved this 8th day of April, 2025 at Wheaton, Illinois.

DEBORAH A. CONROY, CHAIR
DU PAGE COUNTY BOARD

Attest: _____

JEAN KACZMAREK, COUNTY CLERK



Presentation

421 N. COUNTY FARM
ROAD
WHEATON, IL 60187
www.dupagecounty.gov

File #: 25-0966

Agenda Date: 4/1/2025

Agenda #:



DUPAGECOUNTRY

Technology Committee – IT Projects Update



Technology Committee

Technology Projects Update





ERP Systems

What: Implementing new ERP systems to enhance performance and streamline workflows for Finance and HR

Highlights:

- HR/Payroll System (Dayforce) Implementation
 - **Go-live Date: TBD**
 - Actively addressing implementation challenges and moving things forward
 - Hot Issues:
 - Due to privacy and confidentiality concerns, specific items are not listed in this presentation.
 - Detailed issues can be shared with committee members upon request through appropriate channels.
- Finance ERP RFP
 - TBD

Watch Items:

- Timing of Financial ERP RFP launch and integration requirements

ENTERPRISE
RESOURCE
PLANNING





Mainframe Shutdown Project

What: The IT Department will shut down DuPage County's 40-year-old mainframe in 2025

Highlights:

- Timeline Change: **Q2 or Q3 2025**
- Warrants Application: The Warrants application is the sole remaining application on the mainframe. CloudGavel is being implemented and is scheduled to go live in June 2025

Watch Items:

- Remaining Application – **Warrants**
- Mainframe Maintenance Costs – Annual renewals will have to be watched closely
- Anticipated savings in 2025 will not be realized





Additional Project Updates



- Infor Upgrade of Mingle Portal – **COMPLETED**
- MHC/Image Express Server Upgrade – **IN PROGRESS**
- PRMS MFR/OCR 10.0 Upgrade Project – **IN PROGRESS**
- PRMS RFP (Planning Phase) – **IN PROGRESS**
- Operational Excellence Campaign – **IN PROGRESS**
- FOIA Request Tool – **NOT STARTED**





Municipal Tech Roundtable

February Meeting Highlights – Completed



1. Gartner Presentation – Preparing for a U.S. Administrative Change in Government IT
2. Statewide Chief Information Security Officer – An update on the State of IL Cybersecurity initiatives
3. DOJ New Rule on Accessibility Update Collaboration Opportunities Updates
 - Cybersecurity and AI Taskforce
 - Police Records Management System

Next Meeting: Thursday, May 1, 2025





Q & A





DUPAGECOUNTRY

Thank you!
