



AGENDA – Administration Committee

Thursday, October 15, 2026

6:15 PM

- I. Roll Call
- II. Approval of the August 20, 2026 Administration Committee Minutes

RECOMMENDED MOTION: To approve the Minutes of August 20, 2026 Administration Committee Meeting of the DuPage Water Commission.

- III. Resolution No. R-80-26: A Resolution authorizing an Intergovernmental Agreement with the Northwest Suburban Municipal Joint Action Water Agency for advancement of the Lake Michigan Regional Source Water Initiative
- IV. Request for Board Action: Authorizing the Approval of Requisition No. 82853 to Octave Attune EAM for Annual Maintenance Renewal for software maintenance and licensing renewal in the amount not-to-exceed \$68,000.
- V. Request for Board Action: To approve the 2027 Schedule of Board Meetings
- VI. Request for Board Action: Recommendation for the adoption of the updated Information Technology (IT) Policies
- VII. Request for Board Action: To authorize Business-Related Travel Expenses for seven (7) Commission employees to attend the annual Underground Corrosion Short Course at an estimated expense of \$7,700, as included in the FY-25/26 Management Budget.

RECOMMENDED MOTION: To recommend approval of Items 2 through 6 of the Administration committee Report section of the Commission meeting agenda.

- VIII. Old Business
- IX. New Business
- X. Executive Session

RECOMMENDED MOTION: To go into Executive Session to discuss security procedures pursuant to 5 ILCS 120/2(c)(8), to discuss matters related to personnel pursuant to 5 ILCS 120/2(c)(1) and (2), to discuss acquisition of real estate pursuant to 5 ILCS 120/2(c)(5), to discuss the setting of a price for sale or lease of property owned by the DuPage Water Commission 5 ILCS 120/2(c)(6), to discuss pending, probable, or

imminent litigation pursuant to 5 ILCS 120/2(c)(11), and/or to discuss minutes of closed meetings pursuant to 5 ILCS 120/2(c)(21) (Roll Call).

RECOMMENDED MOTION: To come out of Executive Session (Voice Vote).

XI. Adjournment

**Minutes of a Meeting
of the**

ADMINISTRATION COMMITTEE

DuPage Water Commission
600 E. Butterfield Road, Elmhurst, Illinois

August 20, 2026

- I. Commissioner Romano called the meeting to order at 6:15 PM.
Commissioners in attendance: A. Honig, K. Romano, D. Van Vooren, J. Zay
Commissioners absent: S. Greaney
Also in attendance: D. Mundall, P. May
- II. Commissioner Romano asked for a motion to approve the Minutes of the May 21, 2026 Administration Committee Meeting. Commissioner Van Vooren moved, seconded by Commissioner Honig, unanimously approved by a voice vote. All aye, motion carried.
- III. Commissioner Romano asked for a motion to approve Resolution R-64-26, A Resolution Approving Digital Conversion of Historical Commission Documentation by Microsystems, Inc., at a not to exceed cost of \$50,000 for Fiscal Year 26/27. Commissioner Van Vooren moved, seconded by Commissioner Honig, unanimously approved by a voice vote, all aye, motion carried.
- IV. Commissioner Romano asked for a motion to approve Resolution No. R-66-26, A Resolution Approving an Agreement with Metro Strategies Group as Source Water Initiative Communications Consultant, at a not to exceed cost of \$125,000, 30% reimbursable from NSMJAWA. Commissioner Honig moved, seconded by Commissioner Van Vooren, unanimously approved by a voice vote, all aye, motion carried.
- V. Old Business
No Old Business was offered.
- VI. New Business
Chair Romano mentioned the website is near completion.
- VII. Executive Session
No Executive Session was required.
- VIII. Adjournment
Commissioner Honig moved to adjourn the meeting at 6:21 PM, seconded by Commissioner Van Vooren, unanimously approved by a voice vote. All aye, motion carried. Meeting adjourned at 6:21 PM.



Resolution #: R-80-26

Account: 01-60-772500

Approvals: *Author / Manager / Finance / Admin*

PDM - CAP PDM

REQUEST FOR BOARD ACTION

Date: 10/7/2026

Description: **A Resolution Authorizing an Intergovernmental Agreement with the Northwest Suburban Municipal Joint Action Water Agency for advancement of the Lake Michigan Regional Source Water Initiative**

Agenda Section: Administration Committee

Originating Department: Administration

The DWC Source Water Initiative continues to advance and a solicitation is currently pending regarding the important step of selecting the Program Manager for the project. The submittals for Program Manager are due in mid-October; written submittals will be evaluated in early November, followed by interviews with short-listed firms. The intention is to identify a preferred vendor for consideration by the DWC Board of Commissioners in December 2026, and to have a contract in place with the Program Manager in Q1 2027, after which time they can commence their work to advance the project to ensure completion by the termination of the Chicago contract in 2041.

In order to continue to advance the initiative on schedule, it is imperative to establish an IGA between DWC and NSMJAWA which establishes the foundational concepts for the initiative, especially the establishment of cost sharing requirements and managerial roles. Both parties understand that it is neither possible nor prudent to construct an IGA that addresses all matters that will be presented over the next 15 years; rather, the IGA at this time is intended to establish a foundational document that will be amended as the project advances and additional issues come under consideration.

In this regard DWC officials, legal counsel, and staff have worked diligently and directly with NSMJAWA officials to develop a framework to ensure success. These parties have met regularly and collaborated to establish a governance framework that provides confidence to all parties and which seeks to address the primary needs of all. A draft IGA was provided to the DWC Board of Commissioners in August, after which time we received some comments and suggestions regarding a few elements and terminology that are pertinent to near-term considerations. DWC Attorney Luetkehans has coordinated resolution of these items with NSMJAWA legal counsel, and the updated document and a companion summary memo will be transmitted to you under separate cover.

Additional comments were received relative to longer-term issues, such as bonding, commissioning, and operations - which the IGA is not intended to address at this time - but which will be formally addressed in following addenda. In particular, the likely first addendum is expected to address bond and security requirements; DWC will be selecting Bond Counsel this winter which will thoroughly evaluate and prepare bond indentures and ordinances. These documents will be adopted by DWC and an addendum will be attached to the IGA to incorporate all recommended conditions. While this step is not necessary for the selection of the program manager, it will be important as the financial strategy is employed as the project advances. Additional addenda are anticipated for commissioning and operations as adequate information becomes available to address those items.

As the project continues to advance, additional opportunities for consideration and discussion will be provided, at both the committee levels and at the board level. Commissioners are encouraged to continue to reach out to DWC legal counsel and staff with questions and discussion at any time in the process, and updates will be provided on a monthly basis to ensure transparency and to facilitate continued discussion.

Recommended Motion:

It is recommended that Resolution R-80-26 be approved, authorizing an IGA with NSMJAWA for the Lake Michigan Regional Water Supply Initiative.

RESOLUTION NO. R-80-26

A RESOLUTION AUTHORIZING THE EXECUTION OF AN INTERGOVERNMENTAL AGREEMENT
BETWEEN THE DUPAGE WATER COMMISSION AND THE NORTHWEST SUBURBAN MUNICIPAL JOINT
ACTION WATER AGENCY FOR THE LAKE MICHIGAN REGIONAL SOURCE WATER INITIATIVE

WHEREAS, the DuPage Water Commission (the “Commission”) is a county water commission, body politic and corporate, political subdivision, and unit of local government authorized, existing and operating under the Water Commission Act of 1985, 70 ILCS 3720/0.01 *et seq.*, and Division 135 of Article 11 of the Municipal Code, 65 ILCS 5/11-135-1 *et seq.*; and

WHEREAS, the Commission has been studying a Regional Source Water Initiative (the “Initiative”); since 2022 and the studies have concluded that the Initiative is technically feasible and financially viable; and

WHEREAS, the Intergovernmental Cooperation Act (the “Act”), as amended 5 ILCS 220/1 *et seq.*, authorizes units of local government to exercise and enjoy jointly their powers, privileges or authority, and to enter into intergovernmental agreements for that purpose; and

WHEREAS, under the Act, participating units of local government may use their credit, revenues, and other resources to pay costs and to service debt related to intergovernmental activities; and

WHEREAS, Northwest Suburban Municipal Joint Action Water Agency (“NSMJAWA”) was created under the Act to finance, construct and operate a water supply system to serve its member municipalities and other potential water purchasers; and

WHEREAS, DWC and NSMJAWA believe that it is in the best interests of both parties to enter into an Intergovernmental Agreement, for the purposes of economy and adequacy of water supply, under which the Commission and NSMJAWA would jointly construct and operate a joint water supply system to obtain and distribute Lake Michigan water for the use of their respective members and customers; and

WHEREAS, the Commission and NSMJAWA have negotiated an Intergovernmental Agreement to jointly construct and operate a joint water supply system to obtain and distribute Lake Michigan water, a copy of which is attached hereto as Exhibit A; and

WHEREAS, the Commission deems it to be necessary and in the best interests of the Commission and its customers to enter into the Intergovernmental Agreement Between the DuPage Water Commission and the Northwest Suburban Municipal Joint Action Water Agency (the “Intergovernmental Agreement”) attached hereto as Exhibit A, to jointly construct and operate a joint water system with NSMJAWA to provide Lake Michigan water to its customers.

NOW, THEREFORE, BE IT RESOLVED by the Board of Commissioners of the DuPage Water Commission as follows:

SECTION ONE: The foregoing recitals are incorporated herein and made a part hereof as findings of the Board of Commissioners of the DuPage Water Commission.

SECTION TWO: the Board of Commissioners of the DuPage Water Commission hereby approves the Intergovernmental Agreement attached hereto as Exhibit A.

SECTION THREE; General Manager, Paul May, is hereby authorized to execute the Intergovernmental Agreement and take whatever steps necessary to effectuate the terms of said Intergovernmental Agreement.

SECTION FOUR: This Resolution shall be in full force and effect from and after its adoption.

	Aye	Nay	Absent	Abstain
Cuzzone, N.				
Fennell, J.				
Greaney, S.				
Honing, A.				
Noonan, T.				
Novotny, D.				
Pruyn, J.				
Romano, K.				
Russo, D.				
Saverino, F.				
Suess, P.				
Van Vooren, D.				
Zay, J.				

ADOPTED THIS _____ DAY OF _____, 2026.

James F. Zay, Chairman

ATTEST: _____
Danna Mundall, Clerk
Board/Resolutions/2026/R-80-26.docx

EXHIBIT A

INTERGOVERNMENTAL AGREEMENT BETWEEN THE DuPAGE WATER COMMISSION AND THE
NORTHWEST SUBURBAN MUNICIPAL JOINT ACTION WATER AGENCY FOR THE LAKE MICHIGAN
REGIONAL SOURCE WATER INITIATIVE

(TO BE PROVIDED UNDER SEPARATE COVER)



Resolution #: RFBA

Account: 01-60-659000

Approvals: *Author / Manager / Finance / Admin*

JR RCB CAP PDM

REQUEST FOR BOARD ACTION

Date: 10/8/2026

Description: **Authorizing the Approval of Requisition No. 82853 to Octave Attune EAM for Annual Maintenance Renewal**

Agenda Section: Administration Committee

Originating Department: Systems & Information Technology

Staff are requesting authorization to pay Octave Attune EAM (formerly Hexagon) for software maintenance and licensing renewal in the amount not-to-exceed \$68,000.

This expense is for the Enterprise Asset Management (EAM) system, the Commission's Computerized Maintenance Management and Purchasing Management Systems, which has been utilized since 2008. The software maintenance and licensing renewal fee is due annually and in addition to licensing for each staff member, provides the Commission with telephone and online product support, patches, revision changes, and program updates.

This expense is budgeted in the Annual Management Budget, but Board approval is required due to the sole source service provider.

Recommended Motion:

Authorize the General Manager to approve Requisition No. 82853 in the amount not-to-exceed \$68,000 to Octave Attune EAM.

Quote Summary Information

DUPAGE WATER COMMISSION



Service Site : US00161305

Site Contact :

Contact Phone :

Email Address :

Service Address : 600 E BUTTERFIELD RD

City/State/Zip : ELMHURST IL 60126-4642

Country : US

Customer ID : DUPAGE WA/ELMHU US00161305

Bill To Cust : DUPAGE WATER COMMISSION

Bill To Address : 600 E BUTTERFIELD RD

City/State/Zip : ELMHURST IL 60126-4642

Country : US

Policy Number : DDCC550F0

PO Nbr : RENEWAL QUOTE

Service Type : **RENEWAL Q**

Period of Performance : **02/01/2027 - 01/31/2028**

Billed on the : 1 st Day of each period

Period is defined as : Every 12 Months

Previous Cust Code :

Previous Contract # :

Total Contract Value : \$ 67,614.75

*** Totals are exclusive of sales tax. This is NOT AN INVOICE.**

Offered By Octave

Quote: 0000134436

By : _____

Accepted By :
COMPANY _____

Name : Kelly Bergfalk

By : _____

Email : kelly.bergfalk@octave.com

Name/Title : _____

Address : 305 Intergraph Way

POC/Phone : _____

Madison, AL 35758

POC Email : _____

1.864.692.0275

Date : _____

Issue Date : 09/16/2026

Quotes are valid for 90 days from original date of issue. Quote acceptance after 90 days is at the discretion of Octave. Please issue all related purchase orders to Intergraph Corporation.

Messages All services provided hereunder are subject to Octave's Maintenance Service Contract Terms & Conditions (T's & C's) for software (DDCC550F0) unless other specific Terms & Conditions apply and are referenced in the Policy Number field. Copies of the applicable T's & C's may be obtained online at [T's & C's](#). * Totals are exclusive of sales tax - This is NOT AN INVOICE. For coverage code explanations, refer to the last page.

Octave

Quote Summary Information
DUPAGE WATER COMMISSION



Summary Of Service Quote 0000134436

<u>Item Number</u>	<u>Description</u>	<u>QTY</u>
EAM00004	Attune EAM Enterprise Edition for SQL Database NU	41
EAM00014	Attune EAM Enterprise Edition Barcoding NU	1
EAM00016	Attune EAM Enterprise Edition Advanced Reporting Author NU	1
EAM00019	Attune EAM Enterprise Edition Advanced Reporting Consumer NU	41
EAM00035	Attune EAM Enterprise Edition Requestor NU	2
EAM00356	Attune EAM Enterprise Edition Mobile DV	3

Period

Ext Price Summary

2/1/2027 to 1/31/2028

\$67,614.75

Grand Total :

\$ 67,614.75

Quote Summary Information
DUPAGE WATER COMMISSION

**Service Quote Detail**

<u>LI</u>	<u>Sts</u>	<u>Item Number</u>	<u>Description</u>	<u>Site #</u>	<u>Serial Number</u>	<u>Start Date</u>	<u>End Date</u>	<u>Coverage</u>	<u>Cancel Flag</u>
100		EAM00019	Attune EAM Enterprise Edition Advanced Reporting Consumer NU	US00161305	A109497	02/01/2027	01/31/2028	PREM	
300		EAM00014	Attune EAM Enterprise Edition Barcoding NU	US00161305	C109497	02/01/2027	01/31/2028	PREM	
500		EAM00356	Attune EAM Enterprise Edition Mobile DV	US00161305	E109497	02/01/2027	01/31/2028	PREM	
600		EAM00035	Attune EAM Enterprise Edition Requestor NU	US00161305	F109497	02/01/2027	01/31/2028	PREM	
700		EAM00004	Attune EAM Enterprise Edition for SQL Database NU	US00161305	G109497	02/01/2027	01/31/2028	PREM	
800		EAM00016	Attune EAM Enterprise Edition Advanced Reporting Author NU	US00161305	V109497	02/01/2027	01/31/2028	PREM	

Quote Summary Information
DUPAGE WATER COMMISSION



Quote Line Notes:

Coverage Code Definitions:

PREM: Premium Service. A monthly maintenance charge. Includes telephone support, bulletin board support and upgrades when made available by Octave or a Third Party Software Vendor.



Print Requisition



Purchase Requisition

Purchase Requisition 82853 [Octave Attune EAM (formerly Hexagon) Software Maintenance] **Requisition Date** 09/16/2026

Status U [Unfinished]

For Store DPS [DuPage Pumping Station]

Originator 501-0045 [JENESSA RODRIGUEZ]

Date Approved

Services

Line	Task Plan	Due date	Quantity	UOM	Units	Unit Price	Total
1		09/16/2026	1			67,614.75	67,614.75 USD

From Supplier OCTAVEATTUNE [Intergraph Corporation, Octave Attune's Asset Lifecycle Intelligence division]

Work Order - Activity

RFQ

Quotation

Quotation Line

Total **67,614.75 USD**

Approver

Comments

Date

Requisition Comments

RODRIGUEZ [09/16/2026 14:01]:

Annual software maintenance fee for Octave Attune EAM (formerly Hexagon).Copy of original quote is on the Documents tab.Due date: Feb 2027
RFBA will be presented at the October board meeting.
Budgeted under 659000 Computer Software and Licensing



Resolution #: N/A

Account:

Approvals: *Author / Manager / Finance / Admin*

DM - - PDM

REQUEST FOR BOARD ACTION

Date: 10/8/2026
Description: 2027 Schedule of Meetings
Agenda Section: Administration Committee
Originating Department: Administration

Seeking Board approval of the 2027 Schedule of Board and Committee Meetings for calendar year 2027.

Recommended Motion:

To Approve the 2027 Schedule of Meetings.



MEMORANDUM

To: Interested News Mediums

From: Paul D. May, P.E., General Manager

Date: 10/8/2026

Subject: 2027 Schedule of Meetings

As required in 5 ILCS 120/2.03 the following is a list of regular board meetings for the DuPage Water Commission:

January 21, 2027
February 18, 2027
March 18, 2027
April 15, 2027
May 20, 2027
June 17, 2027
July 15, 2027
August 19, 2027
September 16, 2027
October 21, 2027
November 18, 2027
December 16, 2027

The regular Commission meetings begin at **6:30 P.M.**, and are held at the Commission Offices at 600 East Butterfield Road, Elmhurst, Illinois 60126.

The Finance Committee to begin at **5:45 P.M.**, the Engineering and Construction Committee to begin at **6:00 P.M.**, and the Administration Committee to begin at **6:15 P.M.**, prior to the regular Board meetings.



Resolution #: RFBA

Account: N/A

Approvals: *Author / Manager / Finance / Admin*

DC RCB CAP PDM

REQUEST FOR BOARD ACTION

Date: 10/8/2026

Description: **Recommendation for the adoption of the updated Information Technology (IT) Policies**

Agenda Section: Administration Committee

Originating Department: Systems & Information Technology

With the ever-shifting landscape of technology and cybersecurity, the Commission has updated and refreshed the various information technology (IT) policies and combined them into a new IT Policy packet to address emerging issues and best practices. The IT Policy packet includes the combination of the following policies:

- Data Network Policy
- Remote Network Access Policy
- Mobile Device Use Policy
- Password Policy
- Artificial Intelligence Use Policy

The following policies were reviewed and refreshed with updated definitions, guidelines, rules, and requirements included with new systems and best practices. The intent of combining the individual IT Policies into the IT Policy packet is to create a single document that simplifies the cross-policy references and centralizing the related documentation.

The refreshed IT Policies apply to all Commission employees, officers, board members, contractors, representatives, affiliates, agents, and any person or entity performing services for or on behalf of the DuPage Water Commission.

This IT Policy packet has been reviewed by and vetted by Commission Legal Counsel.

Recommended Motion:

To Approve the adoption of the updated IT Policies



DuPage Water Commission

Systems & Information Technology

IT Policies

DuPage Water Commission
600 E. Butterfield Road
Elmhurst, IL 60126
(630) 834-0100

Updated: August 2026

Table of Contents

Data Network Policy	4
1.0 Purpose	4
2.0 Definitions	4
3.0 Policy Statement	5
Remote Network Access Policy	14
1.0 Purpose	14
2.0 Scope	14
3.0 Definition	15
4.0 Policy	16
5.0 Procedures and Guidelines for Access by Third Parties and Their Employees..	17
6.0 Enforcement and Policy Updates	24
7.0 Security Requirements	25
Mobile Device Use Policy	26
1.0 Purpose	26
2.0 Policy	26
3.0 Authorized Device and Controls Table	29
4.0 Prohibited Actions	31
5.0 Rules	31
Password Policy	33
1.0 General	33
2.0 Guidelines	34
3.0 Password Tips For Users	36
Artificial Intelligence Use Policy	41
1.0 Introduction	41
2.0 Definitions	41
3.0 Guiding Principles	42
4.0 Prohibited Uses	44

5.0	Ethical Guidelines.....	46
6.0	Reporting Non-Compliance	48
	Appendix A.....	49
	Employee Consent Form	49
	Appendix B.....	51
	Third Party Consent Form	51

Data Network Policy

1.0 Purpose

The purpose of this policy is to provide Commission employees and other users of the Commission Data Network with guidance regarding the proper use of its electronic Systems. The Commission's mission is to provide quality water services for the Commission customers, and all Commission resources, including its Systems, are to be used in advancing this mission.

1.1 Policy Confidentiality

The contents of the Commission Data Network Policy must be kept confidential and internal to the Commission. The information contained in the policy must be shared only with authorized employees of the Commission, other authorized users of the Commission Data Network, and outside auditors or legal counsel. Disclosure of the contents of the policy, whether intention or accidental, could expose the Commission to increased risk and security breaches as specific information would help a potential intruder exploit known vulnerabilities in selected Systems.

2.0 Definitions

2.1 Commission Data Network

The Commission Data Network includes the Commission's telephone and voicemail systems, fax machines, wireless telephones, mobile devices, radios, computers, electronic mail (e-mail) system, internal computer network, and external computer access (e.g., systems accessing the Internet).

2.2 Confidential Information

All information in the files, whether in electronic or paper form, of the Commission, including but not limited to design, operations and engineering of the Commission's waterworks system and any employee information, regardless of the manner in which it is available, including all copies, reproductions, summaries, analyses or extracts to the extent that they contain such information, is considered "Confidential Information." Confidential Information does not include, however, information which (a) is generally available to the public, (b) was available to the person or the public on a nonconfidential basis.

2.3 Messages

Messages include all communications, oral and in writing, and all files or other data created, uploaded, downloaded, sent, received or stored on any Commission Data Network System.

2.4 Objectionable Content

Objectionable Content includes all content which reasonably could be considered vulgar, offensive, harassing, threatening, obscene, indecent, distasteful, disruptive, defamatory, or derogatory, including but not limited to sexual comments or images, racial slurs, or other comments or images that would offend someone on the basis of his or her race, color, national origin, gender, sexual orientation, religious or political beliefs or disability. This includes any data which is capable of being resolved into Objectionable Content.

3.0 Policy Statement

3.1 Ownership of System and Data

All Commission Data Network Systems and Messages created, received, processed, and/or stored on these Systems are Commission property. All Commission Data Network Systems and Messages are to be used for business purposes only, unless otherwise stated in this Policy.

3.2 Terms and Conditions of Employment

Consent to and compliance with this Policy are terms and conditions of employment for all Commission employees. Failure to fully abide by this Policy, or to consent to any interception, monitoring copying or reviewing of any Messages is grounds for discipline, up to and including termination.

3.3 No Expectation of Privacy

No Commission employee or other user of the Commission Data Network has any right to privacy or other rights with respect to the use of these Systems. Personal and confidential material and information should not be created or stored on the Commission Data Network Systems. Despite systems features that may give the appearance of privacy - including passwords, encryption and the apparent ability to delete messages, Messages are not necessarily private for two reasons:

1. Electronic communications may not be secure. The security of an electronic file on shared systems and networks often approximates that of a document placed in an unsealed envelope - generally respected but easily read by someone determined to do so. Accordingly, employees and users should assume that all Messages may be heard or read by someone other than the intended recipient, that Messages may be altered or intercepted before they reach the intended recipient, and that Messages received may have been altered or sent by someone other than the named sender. Even when a Message is deleted, it still may be backed up elsewhere or it may be possible to recreate the Message.
2. Pursuant to Section 3.4 of this Policy, messages may be audited by the Commission at any time.

3.4 The Commission's Right to Monitor

The Commission reserves the right to monitor the content of all Messages or other information on its Commission Data Network Systems to ensure compliance with this Policy. The Commission also reserves the right to access, retrieve and review all activity and Messages on the Commission's Commission Data Network and to disclose the nature and content of any such activity or Messages to law enforcement officials or other third parties without any prior notice to Commission employees or other involved persons. Employees and other users of the Commission Data Network must cooperate with all reasonable security investigations.

3.5 Files and Message Content

Objectionable Content may not be transmitted or stored on the Commission Data Network Systems. Employees and other users may not knowingly send, receive, cause the receipt of, allow the continued receipt of, or store any information if the information contains any Objectionable Content. No employee or other user may use any Commission equipment or media to bookmark a site or otherwise record the address of an Internet or World Wide Web site that contains Objectionable Content.

If an employee or other user receives Objectionable Content on the Commission Data Network Systems equipment assigned to him or her, the employee or user should immediately contact the General Manager.

3.6 Links to Web Sites

Messages may not contain links to sites that contain Objectionable Content.

3.7 Proprietary Rights and Confidential Information

Employees and other users of the Commission Data Network may not send, post, or divulge confidential information of the Commission outside of the Commission or inside the Commission to unauthorized personnel.

Except for such information that is required for the employee or other user to perform his or her job requirements, use of the Commission Data Network to access any Commission information that is not otherwise routinely available to employees and other users generally is strictly prohibited. In particular, no employee or other user is permitted to access, without the specific authorization of the General Manager, confidential information of the Commission, personal information contained on the Commission Data Network Systems pertaining to other employees, or confidential information of third parties.

3.8 Disrupting Others

No employee or other user of the Commission Data Network may intentionally damage another employee's or user's computer system, disrupt the ability of another to communicate electronically, harass or stalk another, violate the privacy of another, or forge a Message.

3.9 Outside Business Ventures

No employee or other user of the Commission Data Network may use these Systems to conduct any business other than the Commission's business.

3.10 Viruses

Downloading data, information, e-mail attachments, and the like from an outside source increases the risk of viruses and other damaging agents to the Commission Data Network Systems. No employee or other user should retrieve material from outside sources not known to the employee or user unless there are good business reasons for doing so.

Employees and users are permitted to open attachments to e-mail transmissions if they know the source and are expecting the transmission. All other e-mail attachments should be approached with extreme caution.

To further protect the Commission Data Network from computer viruses, no employee or other user may download or install any executable programs or screensavers without the prior approval of a Systems and Information Technology (SIT) Department member.

Employees are responsible for ensuring that appropriate operating system, security software and virus updates and patches are applied at regular intervals to the equipment used to access the network remotely. If the system is used on a daily basis, a check for available updates must be performed daily and when appropriate updates are available, they must be installed immediately.

The SIT Department utilizes a remote management tool to manage security updates on Commission devices. The system will automatically apply updates to the devices, but they may require a reboot. A SIT Department member will send reminders to any employee that has a device that requires a reboot. This task must be prioritized by all employees, so the update can be applied. If the systems are used less frequently, checks for appropriate updates must occur each time that the units are used to access Commission Data Network. The same rules apply to checking updates for:

- Each device's operating system;
- Any application running on the client device that shares data with the host system.

3.11 Internet Browser Default Settings

Browsers used to access the Internet offer varying degrees of security and can be modified by setting options to create greater or lesser degrees of security. No employee or other user may adjust the browser security settings selected by the Commission.

3.12 Compliance with Laws, Regulations, Policies and Professional Business Practices

No employee or other user of the Commission Data Network may knowingly violate any state or federal laws, regulations or the acceptable use policies of any organization through which communications are being made. All Messages created or sent shall be in accordance with professional business practices.

Employees and other users must comply with software license agreements and contracts. Software downloaded from the Internet or bulletin boards must comply with licensing terms and conditions.

3.13 Internet Access and Communications Other Than E-Mail

Unless the General Manager gives prior approval, electronic bulletin boards shall be used solely for Commission business. Participation in any chat groups, electronic bulletin boards, Internet threads, comment forums, instant messaging, hot mail or any other non-e-mail communication may be used only when conducting official Commission business.

Information on the Internet can be fabricated, misleading, malicious or stolen. Viruses may be disguised as programs. There is no guarantee that the information contained in an Internet site has any validity or that the site is sponsored by the entity it purports to be. Simply accessing a site can have damaging effects on the Commission Data Network Systems. Therefore, no employee or other user should access a site of unknown source unless there is a sound business reason for doing so.

Employees are permitted reasonable use of the Commission Data Network to access the Internet for personal reasons. This is a privilege, not a right, and may be withdrawn at any time if abused or if excessive use of the Internet interferes with an employee's assigned job duties. Employees using the Commission Data Network to access the Internet must bear in mind that the Commission may monitor the use of its Data Network Systems, including its systems accessing the Internet. Employees therefore have no expectation of privacy. See Section 3.4, titled "The Commission's Right to Monitor."

Employees are strictly prohibited from uploading, entering, or processing any Commission Confidential Information or source data into unauthorized third-party cloud services, external SaaS (Software as a Service) collaboration tools, or public Generative AI platforms. Refer to the [DWC.Artificial.Intelligence.Use.Policy](#) for additional information.

3.14 Artificial Intelligence Usage

The Commission created and sent out an Artificial Intelligence (AI) Use Policy to all Commission employees in 2026. The policy outlines the Commission's requirements with respect to the adoption of all forms of AI in the organization such as use for organizational efficiencies, operations, and services. The policy outlines the guiding principles, prohibited uses, ethical guidelines, and how to report non-compliance. Refer to the [DWC.Artificial.Intelligence.Use.Policy](#) for additional information.

3.15 Telephone Usage

Employees are permitted reasonable use of the Commission's telephones for personal reasons. This is a privilege, not a right, and may be withdrawn at any time if abused or if excessive use of the telephone interferes with an employee's assigned job duties. Employees using the Commission's telephones must bear in mind that the Commission may monitor the use of its telephones. Employees therefore have no expectation of privacy. See Section 3.4, titled "The Commission's Right to Monitor."

3.16 Electronic Mail

Electronic Mail (e-mail) is made available to employees and Commission board members on the Commission Data Network to facilitate business communications.

Employees and Commission board members of the Commission Data Network should use an appropriate business tone in all e-mail messages. Humor and emotion should not be used because they may not translate well in an e-mail message and could cause misunderstandings for both the sender and the receiver of the message.

Employees, Commission board members, and authorized contactors are permitted reasonable use of the Commission's e-mail system for personal reasons. This is a privilege, not a right, and may be withdrawn at any time if abused or if excessive use of e-mail interferes with an employee's assigned job duties. Employees, Commission board members, and authorized contractors using the Commission's e-mail system must bear in mind that the Commission may monitor the use of its Data Network Systems, including its e-mail system.

All business-related e-mail transmissions inside and outside the Commission has the following "Commission Confidential" disclaimer attached:

- "This e-mail and any of its attachments may contain confidential information belonging or pertaining to the DuPage Water Commission. This e-mail is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this e-mail, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this e-mail is strictly prohibited and may be unlawful. If you have received this e-mail in error, please notify the sender immediately and permanently delete the original and any copy of this e-mail and any printout. Thank You."

3.17 System Security and Configuration Guidelines

The Commission's computers and computer systems are pre-configured with appropriate hardware and software for Commission business use. Installation, changes, or removal of the system hardware or software is prohibited without the approval of the General Manager.

3.18 Passwords

The security for the Commission's computer and voicemail systems includes the use of assigned accounts and passwords. Passwords are intended to protect the employee's or other user's identity and to prevent unauthorized access to protected systems. Employees and other users should take appropriate precautions to ensure the security of their passwords and should not share with another person or keep a written copy of passwords in a visible or obvious location.

Refer to the DWC. Password. Policy for basic guidelines, password protection standards, and password tips.

Remote Network Access Policy

1.0 Purpose

This policy defines the standards and requirements Users must follow when connecting to the Commission Data Network from any host. These standards are designed to minimize the Commission's potential exposure to injury or damages which may result from unauthorized use of Commission resources. Damages include the loss of sensitive or Commission confidential data or intellectual property, damage to the Commission's public image, and damage to critical Commission internal systems, among others. This policy covers both the physical and administrative requirements needed to manage secure network connectivity between the Commission and any third-party requiring access to Commission computing resources.

2.0 Scope

This policy applies to all Commission employees, contractors, vendors, consultants, and agents that use a Commission-owned or personally-owned computer or workstation to connect to the Commission Data Network ("Users"). This policy applies to remote access connections used to do work on behalf of the Commission, including reading or sending e-mail and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to, VPN, SSH, Cloud Access Proxy, SD-WAN Gateway etc.

3.0 Definition

Term	Definition
Remote Commission Access	Any access to the Commission Data Network through a non-Commission controlled network, device or other medium. Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, SSH, cable modems, and other similar access implementations.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: (a) being logged into the Commission Data Network via a local Ethernet connection, and dialing into another Internet service provider (ISP), or (b) being on a Commission-provided Remote Access home network, and connecting to another network, such as a spouse's remote destination.
Split-tunneling	Simultaneous direct access to a non-Commission Data Network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into the Commission Data Network via a VPN tunnel.
VPN	Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

4.0 Policy

These standards are designed to minimize the Commission's potential exposure to injury or damage that may result from unauthorized use of Commission resources. Damages include, but are not limited to, the loss of sensitive or Commission confidential data, or intellectual property, damage to the Commission's public image and damage to critical internal systems. Any User found to have violated this policy or any other Commission policy regarding access to Commission Data Network may be subject to disciplinary action, up to and including termination of employment, or legal action, as appropriate.

4.1 General

It is the responsibility of all Users with remote access privileges to the Commission Data Network to ensure that their remote access connection is given the same consideration as an on-site connection to the Commission.

Access to the Commission Data Network by non-employee Users requires a supervisor's approval and should be limited to business hours (Monday-Friday; 7AM - 3PM CST). Otherwise, the connection will not be established. After the session is over, the connection will be terminated.

Please review the following policies for details of protecting information when accessing the Commission Data Network via remote access methods, and acceptable use of the Commission Data Network:

- a) Mobile.Device.Use.Policy; and
- b) Commission.Data.Network.Policy;

4.2 Requirements

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases. For information on creating a strong passphrase see the Passwords provision (Section 3.17 in the Commission Data Network Policy).

Commission employees and other authorized Users with remote access privileges must ensure that their Commission-owned computer, which is remotely connected to the Commission Data Network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the User.

Commission employees and other authorized Users with remote access privileges to the Commission Data Network must not use non-Commission e-mail accounts (i.e., Gmail, Yahoo, etc.), or other external resources to conduct Commission business, with exception to consultants' business provided e-mail accounts, thereby ensuring that official business is never confused with personal business.

Reconfiguration of a home user's equipment for the purpose of split tunneling or dual homing is not permitted at any time.

No personal equipment is to be used to connect to the Commission Data Network.

5.0 Procedures and Guidelines for Access by Third Parties and Their Employees

5.1 Roles and Responsibilities

The Commission SIT Department will be the primary point of contact regarding requests for third party access to the Commission Data Network.

Third parties bringing computer resources into the Commission and requesting access to the Commission Data Network will require direct authorization from the S/IT Supervisor and/or the Network Administrator. Any third-party connections to the Commission Data Network will require a contract in place and proof of cybersecurity insurance. Third parties will be responsible for any Commission business interruptions or losses should their connection or equipment affect Commission network equipment or systems.

Commission SIT Department (Systems and IT Department):

The SIT Department is responsible for receiving and approving temporary, contractor, consultants, and third-party access privileges and for the review and approval of all third-party access requests. The SIT Department is also responsible for hiring temporaries, consultants or contractors and ensuring that third-party policies or contract terms are understood and followed by all.

The SIT Department also provides setup of connections and single-user VPN connections. The Network Administrator also ensures that properly requested changes to user accounts (for account types that he or she manages) are carried out in an appropriate and timely manner and that required procedures are followed.

Commission Sponsor:

The role of the Commission sponsor is to be the contact point and coordinator in the third party / Commission relationship. The sponsor is also responsible for making sure that third party responsibilities are understood by everyone.

The Commission sponsor of third-party access must promptly notify the SIT Department when access is no longer needed or requires modification. This may include logins, remote access, and permanent connections.

5.2 Temporaries or Contractors

Hired through the recruiting process, temporaries or contractors work in the Commission office:

- Typically they are employed through one of the Commission's lines of business or another temporary service; and
- Use of Commission equipment and resources is standard for this type of third party.

General Policies:

- Temporaries or contractors working onsite for the Commission will be given end-user access unless their job function requires more extensive permissions.
- Accounts expire in 90 days and must be renewed by the third party's sponsor.
- All Commission policies, procedures, standards and guidelines apply.
- Temporaries or contractors requesting remote access must comply with this Remote Network Access Policy and the Commission Data Network Policy.

5.3 Consultants

Consultants are generally from a third-party company with some form of contract or statement of work to be provided to the Commission.

General Policies:

- Consultants may use Commission equipment and are treated like a temporary or contractor with regards to the use of Commission equipment.
- Accounts expire in 90 days and must be renewed by the third party's sponsor.
- The Commission must be notified of any changes in third party personnel. New personnel will be granted access to the Commission Data Network only on an individual basis and according to a specific agreement, not by assuming the identity of the former user.
- All Commission policies, procedures, standards and guidelines apply.
- Consultants requesting remote access must comply with this Remote Network Access Policy and the Commission Data Network Policy.

5.4 Third Party Companies

Third party companies who have a business relationship with the Commission may require technical connectivity to Commission Data Network on a permanent or semi-permanent basis. The following policies apply to third parties.

General Policies:

- Each third-party employee must have his or her own account, and those accounts must not be shared, unless authorized by SIT Department staff. User accounts expire in 90 days and must be renewed by the third party's sponsor.
- The Commission shall be notified of any changes in third party personnel. New personnel will be granted access to the Commission Data Network only on an individual basis and according to a specific agreement, not by assuming the identity of the former user.
- The third-party company shall promptly notify the Commission when any authorized third-party company employee leaves said company's employ or no longer requires access to Commission technology resources.
- All Commission policies, procedures, standards and guidelines apply.
- Third party companies requesting remote access must comply with this Remote Network Access Policy and the Commission Data Network Policy.
- The third-party company shall allow only its employees performing work for the Commission access to the Commission Data Network or to any Commission equipment. The Commission has the right to approve, monitor and restrict all third-party company employees having access to the Commission Data Network. The third-party company is responsible for ensuring that its employees follow Commission policies, procedures, standards and guidelines.
- Commission equipment located offsite at the third-party companies' premises must be secured according to Commission policies, procedures, standards and guidelines.

Notifications:

Third party companies must notify the Commission, via agreed upon methods, (by e-mail, telephone or in writing) promptly:

- Upon any change to the user base for the work performed over the approved third-party network connection; and
- Whenever a change to the connection or the functional requirements of the third-party access connection is necessary.

Network Security for Third Party Company Access:

When there is a business need for a third-party connection, a risk assessment must be carried out to determine security implications and control requirements. An adequate controls strategy must be agreed upon and defined. Access will not be granted until risks associated with the request are discussed and a risk mitigation strategy is agreed upon with the Commission and the request sponsor. The Commission Change Management Process must be adhered to for tracking and implementing change requests associated with the connection (including the initial setup of the connection).

Both the Commission and the third-party companies are responsible for the selection, implementation and maintenance of security procedures and policies that are sufficient to ensure that:

- Access to Commission Data Network and the third-party company's use of Commission-owned equipment is secure and is used only for authorized purposes; and
- The Commission's business records and data are protected against improper access, use, loss, alteration or destruction.

5.5 Third Party Use of Commission Equipment or Software

The Commission may, at its sole discretion, loan to the third-party certain equipment or software for use on the third-party or Commission's premises. An agreement governing the third party's use of the equipment, the term of the loan, and any other applicable restrictions or permissions, will be signed by authorized management at both the Commission and the third party.

Users are responsible for ensuring that appropriate operating system, security software and virus updates and patches are applied at regular intervals to the equipment used to access the network remotely. If the equipment is used daily, a check for available updates must occur daily and when appropriate updates are available they must be installed immediately. If the devices are used less frequently, checks for appropriate updates must occur each time that the units are used to access Commission Data Network. The same rules apply to checking updates for:

- Each device's operating system; and
- Any application running on the client device that shares data with the host system.

Modifications to Commission Equipment:

No modification to the configuration of Commission equipment on the third party or Commission's premises is allowed unless a formal written request is approved in writing by Commission Management. Once an approved modification is completed, the third party must notify the Commission, via agreed upon methods (i.e. by e-mail, telephone or in writing).

5.6 Third Party Use of Non-Commission Equipment on the Commission Data Network

Documented approval and authorization of third-party use of non-Commission equipment is required (refer to the Third Party Access Agreement). If allowed to use non-Commission equipment, Users accessing Commission Data Network must have the following security software installed on their equipment:

- Personal firewall (that limits access to and from the machine);
- Anti-virus (that has both real-time protection and scheduled virus scans); and
- Spyware detection (or equivalent)

Users are responsible for ensuring that appropriate operating system, security software and virus updates and patches are applied at regular intervals to the equipment used to access the network remotely. If the equipment is used on a daily basis, a check for available updates must occur weekly and when appropriate updates are available, they must be installed immediately. If the devices are used less frequently, checks for appropriate updates must occur each time that the units are used to access Commission Data Network. The same rules apply to checking updates for:

- Each device's operating system; and
- Any application running on the client device that shares data with the host system.

Note: Machines may be audited at any time and those found to be non-compliant with these requirements will be denied access to Commission Data Network.

6.0 Enforcement and Policy Updates

Requests for policy exceptions must have valid business justification. The exception must be documented and approved by the system owner or department manager. The Commission will evaluate, approve and store exception requests.

Note: Each exception request must be justified, documented and approved separately. The Commission maintains the right to deny any exception from this policy.

6.1 Enforcement

Network activities may be monitored and logged to ensure compliance with the rules established in this and other Commission policies, procedures, standards and guidelines.

Any User found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, denial of access privileges, legal action as appropriate, or any combination. No provision of this policy will alter the at-will nature of the employment relationship between the Commission and any of its employees.

6.2 Policy Update and Notification

The Commission reserves the right to revise this policy at any time by giving notice.

Users are responsible for understanding or seeking clarification of any rules outlined in this document and for familiarizing themselves with the most current version of this policy.

7.0 Security Requirements

Personal equipment that is used to connect to the Commission Data Network must meet the requirements of Commission-owned equipment for remote access. Reconfiguration of a home user's equipment for the purpose of split tunneling or dual homing is not permitted at any time.

Secure remote access is strictly controlled via one-time password authentication or public / private keys with strong passphrases. For information on creating a strong password or passphrase refer to the DWC Password Policy.

All hosts that have remote access to the Commission Data Network must have an up-to-date version of the Commission provided endpoint protection.

Organizations or individuals who wish to implement non-standard remote access to the Commission Data Network must obtain prior written approval from Commission SIT Department.

Users are responsible for ensuring that appropriate operating system, security software and endpoint protection updates and patches are applied at regular intervals to all hosts that have remote access to the Commission Data Network. Updates and patches are supported by the Commission SIT Department and should be consulted with any questions or assistance.

Mobile Device Use Policy

1.0 Purpose

This policy applies to employees, temporary staff, consultants, contractors and/or vendors employed by or working for the Commission (“Users”). This policy describes the rules covering use of mobile computing Devices that can be attached to the Commission Data Network, or that contain Commission information. This includes, but is not limited to, laptop PCs, tablet PCs, Smartphones, and mobile phones (hereinafter “Devices”).

This policy also is designed to protect the Commission’s resources against intrusion by those who would use wireless media to penetrate the network.

2.0 Policy

All Commission–supplied mobile Devices and their contents remain the property of the Commission and are subject to regular audit and monitoring without notice. Users have no expectation of privacy with respect to communications transmitted to or from or information stored or contained on such Devices, including personally-owned Devices used for Commission business. Such Devices shall only be connected to a computer that has been approved for use at the Commission.

In certain business situations, Users may need to attach non-Commission-owned Devices to a Commission-owned computer or the Commission Data Network. Users may attach non-Commission-owned Devices to the Commission Data Network only under the following circumstances:

- (a) the Device is built to and satisfies all Commission standards for mobile Devices;
- (b) the User obtains authorization from the Systems and Information Technology (SIT) Department to attach the specific Device and the SIT Department has confirmed that the Device and all security settings relating to the Device (passwords, etc.) are configured per Commission standards; and

(c) the User does not change any Device security settings or install any additional programs unless guided by a member of the SIT Department (with the exception of resetting the password and PIN). All program installations and security settings must be done by or with authorization of the SIT Department.

Such Devices shall only be connected to a computer that has been approved for use at the Commission. All Commission information sent to or from or stored in non-Commission-supplied mobile Devices and their contents remains the property of the Commission. Users have no expectation of privacy with respect to non-Commission-supplied mobile Devices that send, receive, or store Commission information or are used for conducting Commission business.

Users shall take appropriate steps to protect Commission-supplied mobile Devices and the Commission information they contain from being lost, stolen or misappropriated. (Refer to table later in this document under section “Personal/Vehicle Laptop.”)

If a Commission-owned Device, or a non-Commission-owned Device attached to the Commission Data Network, is lost or stolen, the User shall contact the SIT Department at (630) 834-0100 ext. 1942 immediately, so that the Commission Data Network can be protected. If the Device is lost or stolen during non-business hours, contact the Commission and the SIT Department’s contact information will be dispensed to the user.

Users shall regularly back up Commission information on any Device to Commission equipment (servers, PC), to protect the data from damage or loss. Where there are security settings held in the Device (such as a Smartphone), Users shall back the Device up to a removable memory Device (such as a USB) or to cloud storage, to ensure that it can easily be reconfigured should complete battery loss cause deletion of the data on the Device (instructions for this will be found in the Device manuals).

Where your Device gets backed up to the Commission Data Network, there is no need to back up to a removable device. The backup on the Commission Data Network will suffice. Ensure that the backup media is securely stored, in a location separate from the Device.

Regular backups of personal data are recommended but not required.

Do not back up data from the Device to non-Commission equipment.

Only applications provided with the Device or provided / approved by the Commission can be run on the Device.

Information that has been classified as Commission Confidential should not be transmitted to or from or stored on mobile Devices unless it is encrypted (where this facility is available on the Device; where it is not, the user must consider carefully before allowing it to be stored on the Device).

All users of mobile Devices are bound by all Commission rules and policies, the Commission Data Network Policy and rules generally applicable to electronic communications apply equally to mobile Devices.

3.0 Authorized Device and Controls Table

Please ensure that your Devices are configured as follows:

Approved Device	Security Requirement
USB Memory Stick	Encrypted if confidential information stored. Commission-owned memory stick shall have the capability of password or PIN control. The password or PIN should be logged with management to ensure the ability to retrieve Commission information should the need arise.
Mobile Device	PIN (mandatory for phone functions) and password (if available). A 4-digit PIN is the minimum acceptable security measure. Some Commission-provided facilities require the use of an 8-digit alpha numeric password.
Mobile Hotspot	A portable device or feature that shares a cellular internet connection with other nearby devices such as laptops, tablets, or cell phones.
MiFi	A small portable wireless router that acts as a mobile Wi-Fi hotspot.
CD/DVD	Files should be password protected (if supported by the hardware). Once used, data should be removed from the CD/DVD and the CD/DVD disposed of appropriately. Data that is not deemed Commission specific (deemed suitable for complete public consumption) may be stored unprotected on the disk. Where data is required to be stored on this media for archive / reference purposes, adequate care must be taken to ensure this data is not disclosed to unauthorized individuals. When data is removed, the CD/DVD must be shredded.

Personal/Vehicle Laptop/Tablet	Strong passwords must be used (See Commission Data Network Policy, 3.17 Passwords). Laptops must be locked in vehicle mounts whenever the laptop is in a vehicle and the vehicle key must be removed. Laptops and Devices shall not be used while driving. Vehicles should be locked when not occupied. If a laptop must be used outside of a vehicle, it must not be left unattended. When not in use the laptop should be turned off or locked out so a password is needed to access information. WIFI, Bluetooth, Windows guest account, and IR port should be disabled. Automatic Windows updates must be enabled as well as Windows firewall and Datto.
Tape	Files should be password protected (if supported by the hardware). Once used, data should be removed from the tape and the tape disposed of appropriately. Data that is not deemed Commission specific (deemed suitable for complete public consumption) may be stored unprotected on the tape. Where data is required to be stored on this media for archive / reference purposes, adequate care must be taken to ensure this data is not disclosed to unauthorized individuals.

4.0 Prohibited Actions

- No changes to the security settings or configuration of any approved Device can be made without prior authorization from SIT.
- Users shall not attempt to use an unapproved Device, via any method of communication, with any SIT equipment that belongs to the Commission.
- Commission staff are provided with mobile hotspots and MiFi's, and they are not to be used aside from the assigned personnel. Mobile hotspots and MiFi's are not to be shared with any third parties.
- Personal mobile phones, with cameras, and personal digital cameras are permitted in the office but must not be used to collect and store data that belongs to the Commission.

5.0 Rules

Specific Points on the Use of Camera Phones:

- Phones enabled with cameras should primarily be used for taking business-related pictures. However, some limited personal use is allowed, but storage must not interfere with Commission business use.
- The prohibition on Objectionable Content in the Commission's Commission Data Network Policy applies to mobile phones as it does to all other forms of electronic communication.
- Information should be downloaded to a secure Device (Commission-owned laptop, for example) and removed from the phone at the users' earliest opportunity.

Specific Points on the Use of Bluetooth-Enabled Devices:

- Bluetooth must only be used for accessing passive devices – such as hands free kits.
- Bluetooth cannot be used to communicate with a Device directly connected to the Commission Data Network (unless through a Commission-owned or leased PC).

- Bluetooth connections must be accepted from other devices with care. Ensure that the recipient is known and agree to connection security criteria in advance.
- Never run a Commission Device in broadcast mode. Various viruses and other schemes are prevalent while in this mode.

Specific Points on the Use of Infrared–Enabled Devices:

- Infrared must only be used for accessing passive Devices. No synchronization should be performed using the interface (unless through a Commission-owned or leased PC).
- Infrared cannot be used to communicate with other Devices, and should be turned off / disabled.
- No Commission data can be sent to other Devices (including Commission-owned Devices) using the Infrared protocol.

Specific Points on the Use of MP3 Players (including iPods):

- Commission content should be stored in linear .wav format. Other departments may select other file types, where quality is less important. Acceptable file formats are wav, MP3, wma, AAC & MXF.
- Users must consider the implications of any rights management included within the Devices selected, to ensure easy sharing of content with independents.
- No additional software should be required to allow the Device to communicate with a Commission desktop PC. Usage of iTunes is restricted at the Commission.

Specific Points on the Use of non-Commission owned Devices:

- Only Devices currently supported as purchased Commission Devices are supported. If the Device requires special software to be incorporated onto the desktop, this is not allowed.
- Before attaching a non-Commission owned Device to the Commission Data Network, the User must obtain written permission through the SIT Department. Permission will be granted only where appropriate to the User's job duties.

Password Policy

1.0 General

1.1 Password Requirements

All domain passwords (tied to the active directory) must be changed every sixty (60) days, and all system passwords (SCADA, Infor, Incode, etc) must be changed every ninety (90) days.

- All passwords must be a minimum of twelve (12) characters and must be:
 - Alphanumeric
 - Contain at least one upper-case letter
 - Contain at least one digit
 - Contain at least one symbol
 - Can not repeat the last five (5) passwords previously used
 - Can not have repeat numbers or letters
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every sixty (60) days.
- All system-level passwords (e.g., root, enable, system admin, application administration accounts, etc.) must be changed every ninety (90) days.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system outside of the Keeper Password Management system which has been provided by the Commission SIT Department.
- If passwords need to be shared, utilize Keeper (the Commission's encrypted password management system)
- All user-level and system-level passwords must conform to the guidelines described below.

2.0 Guidelines

2.1 General Password Construction Guidelines

Passwords are used for various purposes at DWC. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password and local router logins. Since very few systems have support for one-time tokens, (i.e., dynamic passwords which are only used once) everyone must be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than ten characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "<Company Name>", "sanjose", "sanfran" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:~<>?,./)
- Are at least twelve alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

2.2 Password Protection Standards

Do not use the same password for DWC accounts as for other non-DWC access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various DWC access needs.

Do not share DWC passwords with anyone that does not have authorization. All passwords are to be treated as sensitive, confidential DWC information.

List of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them contact the Network Administrator.

Do not use the "Remember Password" feature of applications (e.g., Outlook, Web sites etc.).

If an account or password is suspected to have been compromised, report the incident to the Network Administrator and change all passwords.

NOTE: For additional information and tips for creating strong / complex passwords, please see Appendix A: Password Tips for Users.

3.0 Password Tips For Users

(How to Construct a Complex Password You Can Remember but Hackers Find Hard to Crack)

Your system requires you to use what is called a complex password. By definition, a complex password incorporates at least the following:

- Lower case letters
- Upper case letters
- Numbers (for instance, 1, 2, 3)
- Symbols (for instance, @, =, -, and so on)
- Unicode characters

You will also be required to change your password frequently.

Your system not only forces you to use a complex password, it also checks your password history to make sure you don't use an old password, up to five versions back.

All this can be very frustrating if you don't figure out a good way to create and remember all these new complex passwords. It is very tempting to write your password down in a place you can easily check each morning. However, the minute you do that, unless you are very careful where you store it and who sees it, you've greatly increased the risk of compromising that password. That is why the Commission SIT Department has provided every employee with an encrypted password management system called Keeper. It is a requirement to use this password management system, and the SIT Department team members are always available to provide any additional training, answer questions, or provide support on this system.

This document gives you some tips for figuring out new passwords that meet all the criteria and are still easy for you to remember.

Below is some general advice about Length of Passwords, then Password Basics to keep in mind, and finally Dos and Don'ts.

A NOTE ABOUT LENGTHY PASSWORDS:

Most password cracking tools assume the password will never exceed 14 characters, which is the limit that DOS network boot disks, Microsoft Remote Installation Services (RIS) Pre eXecutable Environment (PXE) boot disks, and older Lan Manager clients (Win9x) must utilize. Even without complexity, a very long password (>14 characters, up to 128 characters) can be the best possible protection against having an especially sensitive password hacked.

For instance, administrators could decide to use a long sentence that is easy to remember, e.g. “You can try and crack this until the cows come home”. Even if more than 14 characters are attempted, the length of this password alone makes the hacker’s task exponentially difficult.

If administrators have legacy systems, RIS, or similar requirements to stick to the 14 character passwords, or simply dislike dealing with an especially lengthy password, (fearing too many typos and lockouts might inadvertently occur) using a shorter password with complex characters offers good protection.

However, keep in mind the longer the password the more difficult it is to crack. And adding both complexity and length makes it the most difficult of all to crack.

Password Basic Tips:

Tip 1: Use More than One Word

For instance, instead of just using the name of someone you know, Allison, choose something about that person no one else knows about, for instance, AllisonsBear or AlliesBear. We’ll add symbols to this to make it complex.

Tip 2: Use Symbols instead of Characters

Many people tend to put the required symbols and numbers at the end of a word they know, for instance, Allison1234. But think about it: this is relatively easy to hack—the word Allison would be in a lot of dictionaries that include common names; once that is discovered, you’ve left the hacker only four more characters to guess (and relatively easy characters, the first guess would probably work).

Instead, drop symbols inside the word in ways you recognize. Most people have their own creative interpretations when it comes to looking at a symbol or number and deciding what it looks like most as a character. As an example, try substituting @ for A, ! for I, a zero (0) for an O, a \$ for an S, a 3 for an E. With those possibilities, @ll!s0nBe@r, A!!is*nBe0r, @//i\$onB3@r are all recognizable, but extremely difficult to hack, even if they are used sequentially. No password dictionary used by hackers can try all these possible combinations and guess at your favorite substitutes for characters easily. Look at the symbols across the top of the numbers on your keyboard and think of the first character that comes to mind—it won't necessarily be what someone else will see in it, but you will remember it.

Tip 3: Choose Events or People That Are On Your Mind

To remember a complex password that is constantly changing, pick something that is on your mind; use this as an opportunity to remind yourself about something pleasant (or unpleasant) that is going on in your life, that few people know about. You won't be likely to forget the password if it is slightly funny or painful, or just plain memorable. Make it unique to you. Be sure to make it a phrase, or at least two words, and continue to slip in your symbols: J0hn\$Gr@du@tion, MyT0eHuRt\$

Tip 4: Use Phonetics in the Words

In general, password dictionaries used by hackers search for words embedded inside your password. As mentioned before, don't hesitate to use the words, but make sure you liberally sprinkle those words with embedded symbols. Another way is to trump that hacking is to avoid spelling the words properly, or use funny phonetics that you remember well. For instance, "Run for the hills" could become R0n4dHiLLs! (if your manager's name is Ron, you might get a laugh each morning typing this in). If you are a lousy speller, you are ahead of the game already.

Tip 5: Don't be Afraid to Make the Password Lengthy

If you remember it better as a full phrase, go ahead and type it in. Longer passwords are much harder to hack. And even though it is long, if it is easy for you to remember, remember you will probably have a lot less trouble getting into your system, even if you aren't the best typist in the world.

Tip 6: Use First Letters of a Phrase

To create an easy-to-remember and strong password, begin with a properly capitalized and punctuated sentence that is easy for you to remember. For example: "My daughter Kay goes to the International School." Next, take the first letter of each word in your sentence, preserving the capitalization used in the sentence. In the example above "MdKgttIS" would be the result. Finally substitute some non-alpha characters for some of the letters in the password. You might use an 'at' sign "@" to replace an "a" or use an exclamation point "!" to replace an upper-case letter "I". After one such substitution the example password above would be "MdKgtt!S" -- a very difficult password to crack yet a password that is easy for you to remember as long as you remember the sentence on which the password is based.

Do's and Don'ts:

Do:

Take two familiar things, then wrap them around a number or special character. Alternatively, alter the spelling to include a special character. In this manner, you get one unfamiliar thing (which makes a good password because it is easy for you and you alone to remember, but hard for anyone else to discover). Examples:

- Phone + 4 + you = Phone4you (or Fone4y0u)
- cat + * + Mouse = cat*Mouse (or cat*Mou\$e)
- attack + 3 + book = attack3book (or @tack3book)

Combine letters, symbols and numbers that are easy for you to remember and hard for someone else to guess.

Create pronounceable passwords (even if they are not words) that are easier to remember, which lessens the need to write your password.

Try out using the initial letters of a phrase you love, especially if a number or special character is included. For example, 4Sa7YaOF might be a good password choice, unless you are known for quoting the Gettysburg Address.

Don't;

Don't use personal information such as derivatives of your user ID, names of family members, maiden names, cars, license tags, telephone numbers, pets, birthdays, social security numbers, addresses, or hobbies.

Don't use any word in any language spelled forward or backward.

Don't tie passwords to the month (in other words, don't use Mayday in May or April-fool in April).

Don't create new passwords that are substantially similar to ones you've previously used.

Artificial Intelligence Use Policy

1.0 Introduction

The DuPage Water Commission (the “Commission”) is committed to full compliance with applicable laws related to the use of artificial intelligence (AI). Additionally, the Commission is committed to the ethical use of artificial intelligence. This Artificial Intelligence Use Policy ("Policy") outlines the Commission’s requirements with respect to the adoption of all forms of artificial intelligence in this organization. Such artificial intelligence adoption includes use for organizational efficiencies, operations, and services.

This Policy is applicable to all Commission employees, officers, board members, contractors, representatives, affiliates, agents, and any person or entity performing services for or on behalf of the Commission. The General Manager, Systems Engineer & IT Supervisor, Network Administrator, and Financial Administrator are responsible for the enforcement of this Policy. All final decisions regarding whether violations of this policy have occurred rest exclusively with the General Manager.

2.0 Definitions

"Artificial intelligence" or "AI" means the use of machine learning technology, software, automation, and algorithms to perform tasks, prepare document and content, and make rules or predictions based on existing datasets and instructions.

"Artificial intelligence system" or "AI system" means software that is developed to be used for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

"Closed AI system" means an AI system where the input provided by one user is used to train the AI model. Input data from the user is isolated from other users, and the data is considered more secure.

"Embedded AI Tools" means AI tools embedded in existing software tools approved and used by the Commission.

"Non-public DuPage Water Commission data" means any information that, if disclosed, could violate the privacy of individuals, employees, government regulations or statutes, or would divulge critical operational data, or could result in financial loss the Commission, or could injure its reputation.

"Open AI system" means an AI system where the input provided by all users is used to train the AI model. Input data from all users is not private and may be revealed to other users.

"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household.

"DuPage Water Commission Representatives" means all Commission employees, officers, board- members, contractors, representatives, affiliates, agents, and any person or entity performing services for or on behalf of the Commission.

3.0 Guiding Principles

The intent of this Policy is to provide general guidance on the use of AI at the Commission so that the Commission can leverage the use of AI as a tool, while ensuring it continues to meet legal obligations, act in an ethical manner, and retain secure information and operational control of our systems. The use of AI at the Commission should never compromise the Commission's core values or introduce undue risk to the organization. Rather, the use of AI at the Commission should be focused on improving the Commission's ability to maintain operational control and enhance the Commission's ability to fulfill its mission.

This Policy is not intended to address every use of AI at the Commission by DuPage Water Commission Representatives. There are certain departments and functions at the Commission that bear more consideration and potential risks. Before using any AI at the Commission, whether for personal reasons, such as writing an email, or more complex business processes, such as analyzing data, employees should consult with their supervisor and/or the Systems and Information Technology Department and seek guidance. Also, please reference Prohibited Uses in Section IV below for situations in which AI may not be used at the Commission, and High-Risk Use of AI Systems in Section VI below for situations in which extreme caution is required when considering using AI.

In addition, there are certain embedded AI Tools used in existing approved Commission software that do not require additional approval for use. For example, the use of Microsoft Word and Gmail, both of which have embedded AI tools to check spelling or grammar. The use of embedded AI Tools in approved software at the Commission is permitted, provided those software tools are aligned with previous general business uses.

When third-party software, services, or contractors are utilized or employed, any AI usage with software used by these parties or services must receive the prior approval by the Systems and Information Technology Department. Consult with the Commission legal counsel by including an AI-specific clause in any vendor or contractor agreements.

The following principles must be followed when considering using an AI system at the DuPage Water Commission:

The use of an AI system should primarily focus on completing departmental goals as directed by your supervisor. Except for the use of an embedded AI Tool in a software system approved for use at the Commission, any use of a new AI System at the Commission must receive prior approval by the Systems and Information Technology Department and the employee's supervisor.

Individuals using an AI system must have expertise in the subject matter for which the AI is used. AI is to be utilized as a tool and is not a substitute for expertise.

All AI-generated content (writing, datasets, graphs, pictures, etc.) must be thoroughly reviewed by an individual with expertise to evaluate such content for accuracy, as well as general proofing and editing. AI-generated content should be viewed as a starting point, not the finished product. Like any content at the Commission, AI-generated content should conform to the look and feel of the Commission's brand and voice.

If the datasets that the AI is using for the purposes of completing job duties are not accurate, then the information AI provides will not be accurate. Accordingly, all employees must make sure that the product AI produces is accurate.

AI systems are trained on data that may contain inherent bias. Users of these systems are responsible for reviewing any AI-produced content for bias and correcting it as necessary. Non-public DuPage Water Commission information must never be put into an open AI system.

DuPage Water Commission representatives must document all AI systems they are utilizing and for what functions. Documentation of specific AI Embedded Tools in an approved, existing software tool when using that tool as intended is not required. Employees are required to discuss the process for tracking the use of AI systems with their department head and the Systems and Information Technology Department before use.

Commission vendors, contractors, consultants, or any person or entity performing services for or on behalf of the Commission must disclose all AI systems they are utilizing and for what functions. No Commission data or information is to be used through AI systems or tools unless authorized by the appropriate members of the Commission.

The use of an AI system must meet any terms of use or contractual limitations. Contractual restrictions or terms of use may restrict the Commission's use of an AI system that would otherwise be legally compliant and ethically sound. For example, an AI system's terms of use may require the use of certain disclaimers in certain use situations or prohibit the use of the AI system to do certain tasks. DuPage Water Commission representatives should have all terms of use or contracts for AI systems reviewed by the Systems and Information Technology Department and the Commission's legal counsel to ensure compliance with contractual obligations in using an AI system.

Approval of an AI system does not eliminate the need for other internal approvals required at the Commission for the use of technology, such as a security review, privacy review, cost review, and spend approval, legal review, human resources review, etc. An AI system should go through the same review and approval process as other hardware/software or services at the Commission. You should also ensure within your division that your supervisor and the Systems and Information Technology Department are aware of the use of the AI system, and have approved any use of the AI system, particularly for AI-generated content that will be relayed externally.

4.0 Prohibited Uses

There are certain uses of AI that are prohibited in the Commission. Unless otherwise approved by the Systems and Information Technology Department and your Supervisor, Commission employees are prohibited from using AI systems for any of the following activities, at any time:

- I. Using AI systems to identify, screen, or categorize employees, candidates for employment, contractors, including using AI to make decisions about employment based on protected class status.

- II. Using AI to make decisions on employee recruitment, hiring, selection for training or apprenticeship, renewal of employment, promotion, discipline, tenure, or compensation, retention, termination, transfer, etc. or to decide terms and conditions of employment that has the effect of subjecting employees to discrimination on the basis of protected classes under the Illinois Human Rights Act, or to use zip codes as a proxy for protected class under the Illinois Department of Human Rights.
- III. Failing to provide notice as required by regulations adopted (if any) by the Illinois Human Rights to an employee that the Commission is using artificial intelligence for the purposes in item ii above.
- IV. Entering customer and employee confidential information, or personal data about any individual into an AI system.
- V. Entering any sensitive information about an individual into any AI system. "Sensitive information" includes medical, financial, political affiliation, racial or ethnic origin, religious beliefs, gender, sexual orientation, disability status, or any other part of a person's life someone would want to keep private.
- VI. Using an AI system to obtain legal advice.
- VII. Using an AI system to make policy modifications and/or decisions.
- VIII. Creating intellectual property that the DuPage Water Commission desires to register and/or holds significant value to the organization.
- IX. Due to the unregulated resources used by the AI engines, their use has been restricted from the Commission's Network. Accordingly, employees are prohibited from installing AI systems on any Commission asset, such as iPhones, iPads, laptops, surfaces and computers. (Ex. Deepseek, ChatGPT)
- X. Entering any of the Commission's Informational Technology (IT) network or operational data.
- XI. Entering any of the Commission's communications infrastructure information or data, including but not limited to cellular, radio, fiber, and Local Area Network (LAN) data.
- XII. Entering any credentials used for Commission systems or related access.

- XIII. Entering any of the Commission's operational technology or control systems data.
- XIV. Entering any of the Commission's financial information or data, including but not limited to financial data from vendors, customers, or employees.
- XV. Entering any of the Commission's metering data or billing information.
- XVI. Entering any of the Commission's Geographical Information System (GIS) information or data.
- XVII. Entering any of the Commission's internal documentation.
- XVIII. Entering any Non-public DuPage Water Commission data or information.

5.0 Ethical Guidelines

The Commission desires to act in an ethical manner when using AI Accordingly, there may be uses of AI that are legally permissible, but which do not meet ethical requirements. Any use of an AI system at the Commission should conform to the following ethical guidelines:

Informed Consent:

Prior to inputting personal information into a closed AI system, ensure that you have obtained informed consent from the individual(s) whose personal information will be inputted.

Integrity in Use:

All users of AI systems must be honest about how AI helped in getting the work done. Even if an employee is using an AI system approved by the Systems and Information Technology Department for an approved use, they must ensure that their manager, or the department requesting a task for which you are using an AI system, is aware of your use of the AI system to accomplish a task.

Do not pass off AI-generated work as done by you solely. Additionally, you should ask permission if you desire to use an AI system tool to complete a task. For example, you should ask your manager and Human Resources Representative if you may use an AI system to assist in writing a performance evaluation.

Appropriate Content:

Employees are prohibited from using Commission time or resources to generate content using an AI system that would be considered illegal, inappropriate, harmful to the Commission's brand or reputation, or disrespectful to others.

Unauthorized Use:

Employees shall not use Commission time or resources to generate content using an AI system for personal use.

General AI System Use Standards and Use Approval:

Except for AI Embedded Tools in approved software, all uses of AI systems must be approved by the employee's supervisor and the Systems and Information Technology Department prior to use to ensure such AI system use meets the following principles:

- ▶ Lawful: The use of AI systems must comply with all applicable laws and regulations, as well as any contractual obligations, limitations, or restrictions.
- ▶ Ethical: The use of AI systems must adhere to ethical principles, be fair, and avoid bias.
- ▶ Transparent: There must be clear objectives for the use of an AI system and documented oversight of such use, which is recorded and captured for institutional knowledge. Disclosures of the use of AI in any AI-assisted content generation must be made when required by law or contract, or when required by the Commission.
- ▶ Necessary: The use of AI systems must be for a valid business purpose to improve Commission business efficiencies and support the organization's mission. The use of AI is not a substitute for human critical thinking or expertise, and should not require the Commission to incur an unnecessary expense without any true benefit.

6.0 Reporting Non-Compliance

Commission managers, supervisors, employees, and agents aware of any conduct that may violate this Policy have a responsibility to report it. Individuals are encouraged to make reports through normal reporting relationships beginning with their supervisor. If the violation involves their manager, the conduct must be reported to the Human Resources Representative, the Systems and Information Technology Department and/or the General Manager. All reports of suspected misconduct or non-compliance will be investigated by the General Manager or his/her designee. Unless acting in bad faith, Commission employees will not be subject to reprisals for reporting potential violations.

If the Commission determines that an employee failed to comply with this Policy after an investigation concludes, then the Commission Representative may be subject to disciplinary action.

Appendix A

Employee Consent Form



DUPAGE WATER COMMISSION
INFORMATION TECHNOLOGY POLICY
EMPLOYEE CONSENT FORM

I hereby acknowledge that I have received a copy of the following DuPage Water Commission Information Technology Policies:

- (a) Data Network Policy
- (b) Remote Network Access Policy
- (c) Mobile Device Use Policy
- (d) Password Policy
- (e) Artificial Intelligence Use Policy

I hereby acknowledge that I have read the provided Policy, and that I understand the terms of the Policy.

I hereby agree to abide by all of the terms and conditions of the Policies. I understand that any failure on my part to comply with any of the terms or conditions of the Policies will subject me to disciplinary action, which disciplinary action could include immediate termination of my employment with the Commission.

Printed Name

Signature

Date

Appendix B

Third Party Consent Form



DUPAGE WATER COMMISSION
INFORMATION TECHNOLOGY POLICY
THIRD PARTY CONSENT FORM

I hereby acknowledge that I have received a copy of the following DuPage Water Commission Information Technology Policies:

(a) Remote Network Access Policy

I hereby acknowledge that I have read the provided Policy, and that I understand the terms of the Policy.

I hereby agree to abide by all of the terms and conditions of the Policies. I understand that any failure on my part to comply with any of the terms or conditions of the Policies will subject me to liability for any damages incurred by the Commission, along with termination of my company's contract with the Commission.

Printed Name

Signature

Date



Resolution #: RFBA

Account: 01-60-613301, 01-60-613200

Approvals: Author / Manager / Finance / Admin

RCB RCB CAP PDM

REQUEST FOR BOARD ACTION

Date: 10/8/2026

Description: Travel and related expenses for seven (7) Commission employees to attend the annual Underground Corrosion/Certification Course in Ft. Wayne, IN

Agenda Section: Administration Committee

Originating Department: Administration

- Underground Corrosion Short Course – This annual conference and training provide the opportunity to gain advanced insight and hands-on skills in corrosion management, support continuous professional growth and expertise, and provide professional development hours to maintain AMPP Cathodic Protection certifications and Professional Engineering licensure.

Dates	Location/Event Description	Budgeted/Estimated	
		Attendees	Expenditure
February 23-25, 2027	Annual Underground Corrosion Short Course – Ft. Wayne IN.	Operations Supervisor Instrumentation Technician Pipeline Supervisor Pipeline Coordinator Pipeline Technician Pipeline Technician Engineering Technician	Estimated at \$7,700 (including Registration, Lodging, Transportation and per diems)

Recommended Motion:

To authorize Business-Related Travel Expenses for seven (7) Commission employees to attend the annual Underground Corrosion Short Course at an estimated expense of \$7,700, as included in the FY-25/26 Management Budget and as listed above.