136 North Monroe Street
Waterloo, WI 53594
Phone: (920) 478-3025
Fax: (920) 478-2021
www.waterloowi.us

PUBLIC NOTICE OF A COMMITTEE MEETING OF THE CITY OF WATERLOO COMMON COUNCIL

Pursuant to Section 19.84 Wisconsin Statutes, notice is hereby given to the public and news media, that a public meeting will be held to consider the following:

COMMITTEE: FINANCE, INSURANCE & PERSONNEL COMMITTEE
DATE: July 17, 2025
TIME: 5:30 pm
LOCATION: Municipal Building Council Chamber, 136 N. Monroe Street

1) CALL TO ORDER AND ROLL CALL

2) APPROVAL OF MEETING MINUTES: June 19, 2025

3) CITIZEN INPUT / PUBLIC COMMENT (3-Minute time limit)

4) OLD BUSINESS
   a) Fire Chief Meeting [NOTES:(1) The committee may convene in closed session per Wis. Stat. 19.85(1)(c) "considering employment, promotion, compensation or performance evaluation data of any public employee over which the governmental body has jurisdiction or exercises responsibility."]
   b) Health Insurance Opt Out Program

5) NEW BUSINESS
   a) June 2025 Financial Statements: Payroll $107,156.81, General Disbursements $148,689.30 and Clerk/Treasurer's Reports [see on municipal website]
   b) 2026 Budget Parameters with Department Heads
   c) Repairs to Water Fountain in City Hall
   d) Resolution 2025-30 Police Vehicle Purchase from Kayser
   e) Fire Protection and Ambulance Service
   f) Handbook changes for Fire Personnel from 53 hours per week to 103 per pay period
   g) Update on Ordinance for Fire Inspection 2025-09 §200-1Fire Inspection and Resolution 2025-10 §200-2 Adoption of WFD Code

6) ROLLING TASK LIST

7) FUTURE AGENDA ITEMS AND ANNOUNCEMENTS

8) ADJOURNMENT

Jeanne Ritter
Clerk/ Deputy Treasurer

Committee Members: Haseleu, Weihert and Kuhl

Posted, Emailed & Distributed: 07/11/2025.

PLEASE NOTE: It is possible that members of and possibly a quorum of members of other governmental bodies of the municipality may attend the above meeting(s) to gather information. No action will be taken by any governmental body other than that specifically noted. Also, upon reasonable notice, efforts will be made to accommodate the needs of disabled individuals through appropriate aids and services. For additional information or to request such services, please contact the clerk's office at the above location.

CITY OF WATERLOO FINANCE, INSURANCE & PERSONNEL COMMITTEE: MEETING MINUTES
June 19, 2025

1. CALL TO ORDER AND ROLL CALL. C. Kuhl called the meeting to order at 6:00 p.m. Members in person: Weihert, J. Haseleu, and Kuhl. Remote: none Absent: none. Others attending in person or remote: Mayor Quimby; Police Chief D. Sorenson; DPW Director Yerges; Utilities Superintendent Sorenson; Fire Chief Butzine; Treasurer Nelson; Clerk Ritter, and WLOO Cable.

2. APPROVAL OF MEETING MINUTES: May 15, 2025 and June 5, 2025. Motion [Weihert/Haseleu] VOICE VOTE: Motion carried.

3. PUBLIC COMMENT (3 Minute Time Limit) none

4. NEW BUSINESS
    a. May 2025 Financial Statements: Payroll $144,080.38, General Disbursements $146,199.85 and
    b. Clerk/Treasurer's Reports [see on municipal website] Motion[Weihert/Haseleu] VOICE VOTE: Motion carried.
    c. Health Insurance Opt Out Program - Discussion

5. OLD BUSINESS
    a. Fire Department-Equipment maintenance contract. Motion to defer until 2026 budget [Weihert/Haseleu] VOICE VOTE: Motion carried.
    b. Job Descriptions for Parks Coordinator – Motion [Weihert/Haseleu] VOICE VOTE: Motion carried.

6. ROLLING TASK LIST
    a. Anti-Bullying /Article II Motion[Weihert/Haseleu] VOICE VOTE: Motion carried.
    b. AI – setting up
    c. Fire Chief Meeting [NOTES:(1) The committee may convene in closed session per Wis. Stat. 19.85(1)(c) "considering employment, promotion, compensation or performance evaluation data of any public employee over which the governmental body has jurisdiction or exercises responsibility."] July 17, 2025

7. FUTURE AGENDA ITEMS AND ANNOUNCEMENTS

8. ADJOURNMENT. MOTION: [Weihert/Haseleu] To adjourn. VOICE VOTE: Motion carried. Approximate time 6:50 pm.

Jeanne Ritter
Clerk/Deputy Treasurer

S&S Plumbing
PO Box 570
Lake Mills, WI 53551-0570

PROPOSAL

Presented to:
City of Waterloo
136 N. Monroe St.
Waterloo, WI 53594-1198

Job #	18281
Job Name	Leaking Water Line at City Hall
Proposal #	P-18281-2
Technician	
Issue Date	Jun 24 2025

Customer Contact:
H: (920) 478-2260
E: jbisco@waterlooutilities.com

Service Location:
136 N. Monroe St.
Waterloo, WI 53594-1198

Price: $690.00

Description	Qty	Price
Remodel We propose to furnish & install the following: - Remove existing remote chiller unit for drinking fountain - Tie water lines together - Existing drinking fountain will be standard cold water temp - Remove and dispose of existing unit - All labor and materials included	1	$690.00

Price **$690.00**

Review and Sign

Customer Approval:

☐ **I accept this proposal and agree to the terms and conditions.**

Contract Terms:

ESTIMATE GOOD FOR 30 DAYS:

- WE RESERVE THE RIGHT TO ADJUST PRICES OF FIXTURES ACCORDING TO ANY UNFORESEEN INDUSTRY COST INCREASES.

***NOTE** If this estimate includes a shower installation, the purchase and installation of a shower door is NOT part of the quote, unless specifically written into the quote at the homeowner's request and acceptance of said quote.*

As soon as fixtures are decided on by the homeowner, we will purchase them right away to avoid any future price increases to the estimate.

Payment Terms:

50% down with signed estimate (an invoice will be sent when we are notified of signed estimate).

Final payment due upon completion of work.

PAYMENT TO BE DETERMINED AS LISTED ABOVE, INTEREST CHARGED AT A RATE OF 1.0% PER MONTH ON ANY OUTSTANDING BALANCES. ANY

LEGAL EXPENSES INCURRED FOR COLLECTION WILL BE AT THE OWNER'S EXPENSE.

Exclusions:

Electrical, carpentry, drywall, tile, tile safing, insulation, patching or painting, wall or floor repair, roof flashing, cutting or drilling counter tops, location or repairs to private underground conduits or utilities, floor scanning or x-ray, concrete cutting or coring, removal or disposal of hazardous or unusable materials, trenching, excavation, select fill, tidewater, frost/rock excavation, temporary water, temporary heat, temporary electric, fire stop or fire protection, high hazard back flow protection, dumpster fees, E&O Insurance, plumbing permits

Notes:
- A 30% restocking charge is applied to all canceled or returned orders
- S&S Plumbing cannot warranty materials provided by others
- Work to be done during normal working hours
- Plumbing permit fees are based on cost per fixture; Permits that are based on total square foot or total job cost are not included
- Concrete more than 4” thick, or concrete with wire mesh/rebar, will be removed on a Time & Materials basis
- Any alterations or deviations from the above specifications involve extra costs executed over and above the original proposal
- All work and materials will conform to the State of Wisconsin Plumbing Codes
- All materials guaranteed to be as specified
- All work completed in a worker-like manner, according to standard practices
- All agreements are contingent upon strikes, accidents, or delays beyond our control
- Owner is to carry fire, flood, and other necessary insurance
- Our workers are fully covered by Worker’s Compensation insurance

Notice of Lien Rights:
As required by the Wisconsin Construction Lien Law, builders hereby notify the owner that persons or companies furnishing labor or materials for the construction on owners’ land may have lien rights on owners’ land and buildings, if not paid. Those entitled to lien rights, in addition to the undersigned builder, are those who contract directly with the owner or those who give the owner notice within 60 days after they first furnish labor or materials for the construction. Accordingly, the owner probably will receive notices from those who furnish labor or materials for the construction, and should give a copy of each notice received to his lender, if any. Builder agrees to cooperate with the owner and the lender, if any, to see that all potential lien claimants are duly paid.

The above prices, specifications & conditions are satisfactory and are hereby accepted. S &S Plumbing is authorized to do the work as specified.

Ed Spiegelhoff, Owner
S & S Plumbing, LLC

S&S Plumbing
PO Box 570
Lake Mills, WI 53551-0570

PROPOSAL

Presented to:
City of Waterloo
136 N. Monroe St.
Waterloo, WI 53594-1198

Job #	18281
Job Name	Leaking Water Line at City Hall
Proposal #	P-18281-1
Technician	
Issue Date	Jun 24 2025

Customer Contact:
H: (920) 478-2260
E: jbisco@waterlooutilities.com

Service Location:
136 N. Monroe St.
Waterloo, WI 53594-1198

Price: $2,950.00

Description	Qty	Price
Remodel We propose to furnish & install the following: - Remove existing chiller for drinking fountain - Install new elkay chiller in same location - Use existing stand and water and power - All labor and materials included	1	$2,950.00

Price **$2,950.00**

Review and Sign

Customer Approval:

☐ **I accept this proposal and agree to the terms and conditions.**

Contract Terms:

ESTIMATE GOOD FOR 30 DAYS:

- WE RESERVE THE RIGHT TO ADJUST PRICES OF FIXTURES ACCORDING TO ANY UNFORESEEN INDUSTRY COST INCREASES.

***NOTE** If this estimate includes a shower installation, the purchase and installation of a shower door is NOT part of the quote, unless specifically written into the quote at the homeowner's request and acceptance of said quote.*

As soon as fixtures are decided on by the homeowner, we will purchase them right away to avoid any future price increases to the estimate.

Payment Terms:

50% down with signed estimate (an invoice will be sent when we are notified of signed estimate).

Final payment due upon completion of work.

PAYMENT TO BE DETERMINED AS LISTED ABOVE, INTEREST CHARGED AT A RATE OF 1.0% PER MONTH ON ANY OUTSTANDING BALANCES. ANY

LEGAL EXPENSES INCURRED FOR COLLECTION WILL BE AT THE OWNER'S EXPENSE.

Exclusions:

Electrical, carpentry, drywall, tile, tile safing, insulation, patching or painting, wall or floor repair, roof flashing, cutting or drilling counter tops, location or repairs to private underground conduits or utilities, floor scanning or x-ray, concrete cutting or coring, removal or disposal of hazardous or unusable materials, trenching, excavation, select fill, tidewater, frost/rock excavation, temporary water, temporary heat, temporary electric, fire stop or fire protection, high hazard back flow protection, dumpster fees, E&O Insurance, plumbing permits

Notes:
- A 30% restocking charge is applied to all canceled or returned orders
- S&S Plumbing cannot warranty materials provided by others
- Work to be done during normal working hours
- Plumbing permit fees are based on cost per fixture; Permits that are based on total square foot or total job cost are not included
- Concrete more than 4” thick, or concrete with wire mesh/rebar, will be removed on a Time & Materials basis
- Any alterations or deviations from the above specifications involve extra costs executed over and above the original proposal
- All work and materials will conform to the State of Wisconsin Plumbing Codes
- All materials guaranteed to be as specified
- All work completed in a worker-like manner, according to standard practices
- All agreements are contingent upon strikes, accidents, or delays beyond our control
- Owner is to carry fire, flood, and other necessary insurance
- Our workers are fully covered by Worker’s Compensation insurance

Notice of Lien Rights:
As required by the Wisconsin Construction Lien Law, builders hereby notify the owner that persons or companies furnishing labor or materials for the construction on owners’ land may have lien rights on owners’ land and buildings, if not paid. Those entitled to lien rights, in addition to the undersigned builder, are those who contract directly with the owner or those who give the owner notice within 60 days after they first furnish labor or materials for the construction. Accordingly, the owner probably will receive notices from those who furnish labor or materials for the construction, and should give a copy of each notice received to his lender, if any. Builder agrees to cooperate with the owner and the lender, if any, to see that all potential lien claimants are duly paid.

The above prices, specifications & conditions are satisfactory and are hereby accepted. S &S Plumbing is authorized to do the work as specified.

Ed Spiegelhoff, Owner
S & S Plumbing, LLC

136 North Monroe Street
Waterloo, WI 53594
Phone: (920) 478-3025
Fax: (920) 478-2021
www.waterloowi.us

Resolution 2025-30

A Resolution of the City of Waterloo Authorizing the Purchase of a New 2025 Ford Police Vehicle

WHEREAS, the Waterloo Police Department needs a new Police Vehicle; and

WHEREAS, bids have been received from numerous dealers; and

WHEREAS, the Police Chief recommends the bid from Kayser in Madison, WI be accepted; and

WHEREAS, the total amount of the new 2025 Ford Police Vehicle is $45,349.84; and

WHEREAS, the funds for this purchase will come from 2025 Police Safety Outlay Equipment.

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Waterloo that:

1. The City Council approves bid from Kayser in Madison, WI. For the purchase price of $45,349.84.
2. This Resolution shall take effect immediately upon passage.

PASSED AND ADOPTED this ____ day of _____ 2025.

City of Waterloo

Signed: _____
Jenifer Quimby, Mayor

Attest:

_____
Jeanne Ritter Clerk/Deputy Treasurer

AGREEMENT FOR FIRE PROTECTION AND AMBULANCE SERVICE

THIS AGREEMENT (the "**Agreement**") is entered into effective as of the last date of signature below, by and between the City of Waterloo, a Wisconsin municipal corporation, existing pursuant to Chapter 62 of the Wisconsin Statutes, (the "**City**"), and the Town of Waterloo, a Wisconsin town existing pursuant to Chapter 60 of the Wisconsin Statutes (the "**Town**").

WHEREAS, sections 60.55, 61.65 and 62.13 of the Wisconsin Statutes authorize the City and Town to provide fire protection and rescue services; and

WHEREAS, section 66.0301 of the Wisconsin Statutes authorize the City and Town to enter into contracts with each other for the furnishing of services and/or the joint exercise of any power or duty required or authorized by law; and

WHEREAS, the City and Town desire to provide for the provision of fire protection and rescue services on a cost effective and efficient basis; and

WHEREAS, the Town desires to promote and make available adequate and reliable fire protection and ambulance services to persons within the boundaries of the Town, and which primary services are described below and are covered by this Agreement; and

WHEREAS, the City is willing to provide fire protection and ambulance services within the Town in accordance with the terms and conditions set forth in this Agreement.

NOW, THEREFORE, in consideration of the mutual promises and covenants of each other contained in this Agreement, and other good and valuable consideration, the receipt and sufficiency of which is hereby mutually acknowledged, the parties agree as follows:

1. DEFINITIONS. Except as otherwise specifically defined in this Agreement, the following terms shall have the following meanings:

a. "**Emergency Medical Technician**" or "**EMT**" has the same meaning as chapter 256 of the Wisconsin Statutes.

b. "**Fire Chief**" means the chief of the Fire Department.

c. "**Fire Department**" means Waterloo Fire and Rescue.

d. "**Fire and Ambulance Services**" or "**Services**" means fire prevention services, fire protection services, and related services, including structural firefighting, fire suppression, rescue, hazardous materials operational level response, fire code inspection and enforcement, fire code, confined space operational level response, preconstruction building plan review, fire investigation, vehicle extrication, basic life support, emergency medical services as set forth in Chapter 256 of the Wisconsin Statutes, public education about fire prevention and safety, and fire cause and origin determination.

e. "**Primary Service Area**" has the same meaning as chapter DHS 110 of the Wisconsin Administrative Code.

2. SERVICES.

a. The City agrees to provide to the Town Fire and Ambulance Services to all persons in need of such Services within the primary service area set forth in Exhibit A (the "**Primary Service Area**"). Emergency medical services shall be provided at the following level:

1. Advanced Emergency Medical Service (Technician Level);
2. Basic Emergency Medical Service (Basic Emergency Medical Technician)

b. The City, through the Fire Department, shall provide Fire and Ambulance Services to the Town, including the furnishing of necessary fire protection apparatus, ambulances, and personnel. The equipment and personnel responding to any call shall be at the discretion of the Fire Chief; provided, that in the event of an emergency within the City, or within another township being likewise served for fire and ambulance service by the City, or for other good reason, the Fire Chief in his/her discretion and in good faith may order a portion of the apparatus and personnel to respond to such other township or to the City. The extent of the obligation of the City herein is that the City will make reasonable efforts to provide Fire and Ambulance Services to the Primary Service Area in the Town, subject to the reasonable need to respond to other incidents, as determined by the Fire Chief.

c. The Fire Department shall have and retain full control, authority, and ownership of the fire fighting and ambulance equipment, and shall have full responsibility for the storage, maintenance, and repair to said fire fighting and ambulance equipment.

d. The Town shall take all reasonable action to provide fire prevention and minimize unnecessary ambulance calls in the Town, and to implement all reasonable recommendations of the Fire Department with respect to such action.

e. The Town agrees the City will be the primary provider of Fire and Ambulance Services within the Primary Service Area, and that the City shall be the first Fire and Ambulance Services provider to be called upon to provide Services within said Primary Service Area. The Town shall not enter into any other agreements for the provision of Fire and Ambulance Services within the Primary Service Area during the term of this Agreement.

3. INSURANCE. The City shall obtain and maintain policies of liability insurance, worker's compensation insurance, and insurance covering the fire fighting and ambulance equipment and its personnel, in amounts and coverages determined appropriate by the City. The City shall promptly provide certificates of insurance to the Town upon request.

4. STANDARD OF CARE. The City shall provide ambulance and emergency medical services, consistent with the standards set forth in Chapter 256 of the Wisconsin Statutes. The City's standard of care shall be that of Advanced Emergency Medical Technician (A License) for the City's primary emergency medical services unit. In the event that the City is required, as reasonably determined by the City, to utilize a second unit, the standard of care shall be that of a

Basic Level Crew. The Fire Chief shall have the discretion to allocate resources as deemed the best interest of the Parties.

5. EQUIPMENT AND PERSONNEL. In providing Fire and Ambulance Services, the fire apparatus and ambulances utilized by the City shall be properly approved and licensed by the State of Wisconsin. Such apparatus and equipment shall be owned by the City, and such apparatus attendants shall be employed by the City. The City shall maintain all vehicles and equipment in good working order as required by law. The City shall maintain all necessary licenses for operation of the Fire and Ambulance Services. All fire fighters and emergency medical technicians functioning as attendants shall be licensed or certified by the State of Wisconsin. All Ambulances shall have the required minimum staffing as established in chapter 256 of the Wisconsin Statutes to comply with the terms of their license issued by the Department. All Ambulances shall at all times carry equipment, supplies, and medications sufficient to meet or exceed the requirements of Chapter Trans 309 of the Wisconsin Administrative Code.

The Fire Department shall comply with the provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

6. COMPENSATION.

A) Aggregate Value Based on current coverage value for Fire and EMS. Allocated on the basis of the total equalized assessed valuation in the area served, and in the manner set forth on the attached exhibits

B) (Additional EMS Coverage Only) In consideration of the services to be provided herein to the Town by the City, the Town shall compensate the City at the per capita rate specified in Exhibit B (the "**Compensation Schedule**") multiplied by the number of Town residents that live within the Primary Service Area (but outside the current Waterloo Fire Department response area), as determined by the Town Clerk from Jefferson County records, and the annual sum due will be set accordingly. Such population determination shall be made after June 1, but before July 1 of each year and conveyed by the Town Clerk to the City Clerk, and in the same manner each and every year thereafter that this Agreement remains in effect. One-half (1/2) of the annual sum shall be paid to the City on or before the subsequent February 1 of each year, and the remaining one-half (1/2) of the annual sum shall be paid on or before August 1 thereafter of each year.

Payments made under this paragraph shall be deemed to be for the calendar year in which the same is paid. These payments are in the form of a non-refundable subsidy in consideration of the City providing the services to the population residing within the Primary Service Area.

7. PATIENT BILLING AND COLLECTION. The Fire Department shall be solely responsible, at its sole cost, for all patient billing and collection. The Fire Department shall comply with all Medicare, Medicaid, and other applicable regulations regarding appropriate billing information, and provide services hereunder in compliance with all applicable federal, state, and County ordinances, rules and regulations.

8. TERM. The initial term of this Agreement shall be for three (3) years, commencing on and terminating at midnight,
. The Agreement shall automatically renew thereafter for subsequent one (1) year terms,

unless notice is given by either party to nonrenewal at least 120 days prior to expiration of said term

9. NOTICE TO CURE BREACH. If either party violates any terms of this Agreement, when such breach becomes known to the other party or reasonably should have become known with reasonable diligence, the party shall provide the other with notice of such breach as provided below. The breaching party shall cure any breach no later than sixty (60) days after the giving of such notice by the other. If the cure is not timely effectuated, then the party sending notice may terminate this Agreement by giving a notice of termination of at least sixty (60) days, as provided above. In addition to termination, the non-breaching party may also pursue any other remedies available to it under law. In the event litigation, the party which substantially prevails in such litigation shall recover in addition to any monetary damages, its costs and expenses in pursuing such litigation, including reasonable attorney fees.

If the breach is for failure to pay any monetary amounts due under this Agreement, the above right to cure shall be reduced to five (5) days. Upon failing to timely cure a failure to pay, the City may immediately cease providing service under this Agreement.

10. DISPATCH. The Town shall immediately forward to the City, at no cost to the City, all "9-1-1" emergency and non-emergency calls. The Town shall use the existing "9-1-1" system already in place at Jefferson County Emergency Dispatch Center to do so.

11. MISCELLANEOUS.

a. Non-Assignability. This is a personal service agreement between the Town and the City. The City may not assign any of the obligations or rights (other than the right to receive the compensation) contained in this Agreement to any other party, without the prior written consent of the Town.

b. Notices. Any written notice or demand hereunder shall be in writing and shall be served by ordinary mail, personal delivery, certified mail, return receipt requested. Notice shall be deemed given when either personally delivered, or if mailed, the third business day after such notice is mailed.

c. Service of Notices. Such notices shall be served or mailed as follows:

To the City:

City Clerk
136 North Monroe Street
Waterloo WI. 53594

To the Town:

Town Chair

d. Amendment. This Agreement sets forth all of the promises, inducements, agreements, conditions and understandings between the parties hereto relative to the subject matter thereof, and there are no promises, agreements, conditions or understandings, either oral or written, expressed or implied, between them, other than as herein set forth. Except as herein otherwise provided, no subsequent alteration, amendment, change or addition to this Agreement shall be binding upon the parties hereto unless authorized in accordance with law, in written amendment and properly executed by the City and the Town.

e. Severability. If any section, subsection, sentence, clause, phrase or portion of this Agreement is for any reason held invalid or unconstitutional by any court of competent jurisdiction, such portion shall be deemed a separate and distinct and independent provision and such holding shall not affect the validity of the remaining portions thereof.

f. Waiver. Neither party shall be excused from complying with any of the terms and conditions of this Agreement by any failure of the other party upon one or more occasions to insist upon or seek compliance with any such terms and conditions.

g. Force Majeure. If performance of any covenant to be performed hereunder by any party is delayed as a result of circumstances which are beyond the reasonable control of such party, which circumstances may include, but are not limited to, acts of God, war, acts of civil disobedience, harsh weather, strikes or similar acts, the time for such performance shall be extended by the amount of time of such delay.

h. Governing Law. This Agreement shall be construed, interpreted and enforced in accordance with the laws of the State of Wisconsin. The Parties shall at all times observe and comply with all federal, state and local laws, regulations and ordinances which are in effect, as of the date hereof, which may affect the conduct of the services to be provided under this Agreement.

i. Indemnification. The City and Town agree to indemnify, hold harmless and defend the other party, its elected and appointed officials, officers, employees and agents from any and all claims, suits, damages, losses, and expenses, including but not limited to reasonable attorney's fees, arising out of or resulting from the indemnifying party's performance of, or failure to perform, the activities provided under this Agreement, but only to the extent caused in whole or in part by the negligent acts or omissions of the indemnifying party, or anyone acting under its direction or control, or on its behalf.

j. No Partnership. Nothing in this Agreement shall be construed to create any co-partnership, principal and agent, joint venture or other similar relationship between the parties hereto and no party may incur debts or liabilities in the name, or on behalf, of any other party unless expressly approved by the party to be bound thereby in a written instrument signed by such party.

k. Nonwaiver of Governmental Immunity. Notwithstanding any provision to the contrary contained herein, no provision of this Agreement shall be construed as a waiver of any immunity or limitation of liability granted to or conferred upon any party by applicable provisions of Wisconsin law.

l. No Third-Party Beneficiaries. This Agreement is intended solely to regulate the obligations of the parties hereto with respect to one another. Nothing in this Agreement is intended to create, admit or imply any liability to any third-party nor to provide any benefit to any person, firm, corporation or governmental or non-governmental entity not a party to this Agreement.

m. Counterparts. This Agreement may be executed electronically and in counterparts, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument.

n. Neutral Construction. The parties acknowledge that this Agreement is the product of negotiations between the parties and that, prior to the execution hereof, each party has had full and adequate opportunity to have this Agreement reviewed by, and to obtain the advice of, its own legal counsel with respect hereto. Nothing in this Agreement shall be construed more strictly for or against either party because that party's attorney drafted this Agreement or any part hereof.

o. Public Records Law. Each party herein shall reasonably cooperate with the other parties herein to facilitate compliance with the Wisconsin Public Records Law, sec. 19.21, et seq., Wis. Stats., and upon request by any other party, provide to the requesting party all documents in their possession or control which are subject to release under such law.

THE FOLLOWING EXHIBITS ARE ATTACHED AND INCORPORATED HEREIN:

Exhibit A: Primary Service Area
Exhibit B: Compensation Schedule

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Agreement effective as of the last date of signature below.

CITY OF WATERLOO

BY: _____ _____
Jenifer Quimby, Mayor Date

ATTEST: _____ _____
Jeanne Ritter, Clerk Date

TOWN OF WATERLOO

BY: _____ _____
, Town Chair Date

ATTEST: _____ _____
, Town Clerk Date

EXHIBIT A
Primary Service Area

EXHIBIT B

Compensation Schedule

In accordance with Section 6 of this Agreement, the Town shall compensate the City at the per capita rate specified below:

Year	**Amount**
2026	**$___30/per capita**
2027	**$___32/per capita**
2028	**$___33/per capita**

§ 200-1. Fire Inspectors.

A. Fire Chief to be Fire Inspector. The Fire Chief shall hold the office of Fire Inspector with power to appoint one or more Deputy Fire Inspectors, who shall perform the same duties and have the same powers as the Fire Inspector.

B. Inspection duties. The Fire Inspectors shall inspect, semiannually, all public buildings and places of employment, as defined in § 101.01(11), Wis. Stats., within the City limits for the purpose of noting and causing to be corrected any conditions liable to cause fires. Repairs or alterations necessary to remove the hazardous condition shall be made within a reasonable time at the expense of the owner. The Inspector shall also investigate the storage and handling of explosives and inflammable liquids within the City.

C. Procedure. Fire inspection procedures and forms shall be developed in accordance with § 101.14, Wis. Stats., and applicable codes of the National Fire Prevention Association.

D. Written record of inspections. The Chief shall keep a written record card of each property inspected which shall conform to the requirements of the State Department of Commerce and shall make the semiannual report of inspections required by said Department.

E. Correction of fire hazards. When any inspection by the Fire Chief or his deputies reveals a fire hazard, the Chief or his deputies may serve a notice, in writing, upon the owner of the property giving said owner a reasonable time in which to remove the hazard. If the fire hazard is not removed within the time allowed it shall be deemed a nuisance, and the Fire Chief or his deputy may have the same removed by the City, and the cost of such removal shall be recovered in an action by the City against the owner of the property and may also be entered on the tax roll as a special charge against the property.

F. Entering on premises. No person shall deny the Fire Inspector or his deputies free access to any property within the City at any reasonable time for the purpose of making fire inspections. No person shall hinder or obstruct the Fire Inspector in the performance of his duty or refuse to observe any lawful direction given by him.

§ 200-2. Adoption of Administrative Code provisions.

A. The following chapters of the Wisconsin Administrative Code, Rules of the Department of Commerce, are hereby adopted by reference and made a part of this Code:

COMM 2	Fee Schedule
COMM 7	Explosive Materials
COMM 10	Flammable and Combustible Liquids
COMM 14	Fire Prevention
COMM 32	Public Employee Safety and Health
COMM 40	Gas Systems
COMM 61 to 65	Commercial Building Code

B. A copy of the above codes is on file in the office of the Fire Chief.

§ 200-3. Accidental spills of hazardous substances.

See Chapter 215, Hazardous Substances, of this Code.

§ 200-4. Burning regulations. [Amended 7-11-2019 by Ord. No. 2019-06]

A. Outdoor burning prohibited. No person shall cause, allow or permit outdoor burning of refuse, garbage, plant life, leaves or other combustible material within the City, except as permitted under Subsection C.

B. Incinerators prohibited. It shall be unlawful for any person to operate and maintain or cause to be operated and maintained any incinerator within the City, except as permitted under Subsection C.

C. Exceptions:

(1) Outdoor burning in connection with the preparation of food.

(2) The burning of refuse in a properly designed, operated and maintained incinerator, duly licensed by the Wisconsin Department of Natural Resources to be effective for the purpose of air pollution control, or outdoor burning by the City of Waterloo pursuant to a permit by the Wisconsin Department of Natural Resources.

(3) Small outdoor flames for welding, acetylene torches, safety flares, heating tar or similar applications.

(4) Any outdoor burning for which a person has obtained a permit from the Waterloo Fire Department.

(5) A fire set for the purpose of training public or private fire-fighting personnel.

(6) A fire set or required by a public officer for the abatement of nuisances and which is necessary in carrying out public health functions.

D. Permit required. A one-time inspection for any new permanent installation of a fire pit (bricks and mortar, concrete, etc.) is required. **[Amended 4-18-2024 by Ord. No. 2024-11]**

E. Responsibilities. The resident shall have the following responsibilities: **[Amended 4-18-2024 by Ord. No. 2024-11]**

(1) To adhere to all health and fire prevention codes.

(2) To have adult (18 years of age or older) supervisory personnel present at the site of the outdoor burning.

(3) To comply with the following conditions:

(a) Any fire deemed to be a public health nuisance by the Fire Chief or his or her designee shall be extinguished.

(b) This shall apply to all manufactured burning rings, fireplaces, fire pits, chimneys or like devices.

(c) No manufactured device shall be placed on any combustible surface.

(d) The fire must be completely extinguished before the fire location may be left unsupervised.

(e) The fire shall be no larger than four feet in diameter, subject to the exceptions listed below.

(f) No flammable liquids shall be used to start or support the burning.

(g) Only virgin wood and charcoal fuel will be allowed to be burned. "Virgin wood" means wood and other wood products, such as bark, but not to include sawdust, which have had no chemical treatments or finishes applied.

(h) Under no circumstances shall plastics, trash, garbage, oils, hydrocarbon fuels, furniture, fabrics, leaves, yard waste, synthetic materials of any kind, pressure-treated wood or wood that has been finished with paints, varnishes, laminates or a similar finish be burned. Burn barrels are not allowed within the City limits.

(i) The fire shall be located at least 10 feet from property lines and at least 20 feet from any building or structure. This does not apply to manufactured devices.

(j) A functional extinguishing aid must be present, such as a fire extinguisher, garden hose, etc.

(4) Exceptions. A bonfire exceeding the size restrictions set forth in Subsection E(3)(e) will be permitted for churches, organized schools, and civic organizations and only if application for site review has been made and approved by the Waterloo Fire Department. Such bonfire shall be no more than 10 feet in diameter or 10 feet by 10 feet square and no more than six feet high and must comply with all other provisions of the permit.

F. Emergency provisions. Notwithstanding any other provision of this section, the Fire Chief, in times of extreme dryness or drought, deficiency in the water supply or by reason of any other emergency, is authorized to prohibit the setting of any fires upon any lands within the City by providing published notice of the declared emergency. Public notice will be made by City-wide call (Connect final site) as well as website and social media. **[Amended 4-18-2024 by Ord. No. 2024-11]**

§ 200-5. Fire prevention rapid entry requirement; Knox-Box systems. [Added 11-7-2019 by Ord. No. 2019-07[1]]

A. Definition. The term "Knox-Box®" shall be defined as a lock box from the Knox Company which allows emergency responders to gain access to secured buildings and perimeters without forceful entry.

---

1. **Editor's Note: This ordinance also renumbered former § 200-5 as § 200-6.**

B. Buildings subject to this section.

(1) The following structures shall be equipped with a Knox-Box® at or near the main entrance or such other location approved by the Fire Chief or designee:

(a) Commercial or industrial structures protected by an automatic alarm system or automatic suppression system, or such structures that are secured in a manner that restricts access during an emergency.

(b) Multifamily residential structures with Four or more units that have restricted access through locked doors or have a common corridor for access to the living units.

(c) Governmental structures as required by the Fire Department.

(d) Nursing care facilities.

(e) All public and private educational facilities.

(2) All newly constructed structures subject to this section shall have the Knox-Box® installed and operational prior to the issuance of an occupancy permit.

C. Buildings requiring a Knox-Box® shall be subject to numbering or lettering. All buildings over 5,000 square feet and with more than two doors must number or letter their doors (and windows when required by the Fire Chief or his/her designee). Numbering/Lettering must be no less than eight inches in size, reflective and a contrasting color to the door. Numbers/ Letters shall be placed on each door starting at the main entrance and progressing around the building clockwise. Numbers/Letters must be at least five feet above ground level. Where double doors or a grouping of doors exists close together, they may be numbered as one.

D. Contents.

(1) The owner or operator of a structure required to have a Knox-Box® shall, at all times, keep keys in the box that will allow for access to the following:

(a) Keys to locked points of ingress or egress, whether on the interior or exterior of such buildings.

(b) Keys to locked mechanical rooms.

(c) Keys to elevator controls.

(d) Keys to rooms containing fire control systems.

(e) Keys to other areas as directed by the Fire Chief.

(2) Each key shall be legibly labeled to indicate the lock that it opens in such a manner as is approved by the Fire Chief or his/her designee.

(3) A floor plan of the rooms within the building may be required at the discretion of the Fire Chief or his/her designee.

E. Compliance. After the effective date of this section, all newly constructed buildings, not yet

occupied, or buildings currently under construction and all buildings or businesses applying for an occupancy permit shall comply. Existing buildings that are not in compliance on the effective date of this section shall comply with requirements of this section within 16 months of this effective date of this section. Any person who owns or operates a structure subject to this section shall be subject to the penalties set forth in Subsection H of this section for any violation of this section.

F. Rules and regulations. The Fire Chief or his/her designee shall be authorized to implement rules and regulations for the use of the lock box system.

G. Brand. The "Knox" brand will be the only lock box permitted by the City of Waterloo.

H. Penalties. Except as otherwise specifically provided in this chapter, any person who shall violate any provision of this section or any order, rule or regulation made hereunder shall be subject to a forfeiture as provided.

(1) First offense shall be a forfeiture of $50 plus court costs and penalty assessments.

(2) Second offense shall be a forfeiture of $100 plus court costs and penalty assessments.

(3) Third and subsequent offenses shall be a forfeiture of $200 plus court costs and penalty assessment.

§ 200-6. Violations and penalties.

Any person who shall violate any provision of this chapter or any order, rule or regulation made hereunder shall be subject to a penalty as provided in Chapter 1, § 1-4 of this Code.

136 North Monroe Street
Waterloo, WI 53594
Phone: (920) 478-3025
Fax: (920) 478-2021
www.waterloowi.us

ORDINANCE #2025-09

An Ordinance Amending Section §200-1

The Common Council of the City of Waterloo, Wisconsin do ordain as follows:

Section 1: § 200-1 **Fire Inspection.**

A. Fire Chief to be Fire Inspector. The Fire Chief shall hold the office of Fire Inspector with power to appoint one or more Deputy Fire Inspectors, who shall perform the same duties and have the same powers as the Fire Inspector.

B. Inspection duties. The Fire Inspectors shall inspect, semiannually, all public buildings and places of employment, as defined in § 101.01(11), Wis. Stats., within the City limits for the purpose of noting and causing to be corrected any conditions liable to cause fires. Repairs or alterations necessary to remove the hazardous condition shall be made within a reasonable time at the expense of the owner. The Inspector shall also investigate the storage and handling of explosives and inflammable liquids within the City.

C. Procedure. Fire inspection procedures and forms shall be developed in accordance with § 101.14, Wis. Stats., and applicable codes of the National Fire Prevention Association.

D. Written record of inspections. The Chief shall keep a written record card of each property inspected which shall conform to the requirements of the State Department of Commerce and shall make the semiannual report of inspections required by said Department.

E. Correction of fire hazards. When any inspection by the Fire Chief or his deputies reveals a fire hazard, the Chief or his deputies may serve a notice, in writing, upon the owner of the property giving said owner a reasonable time in which to remove the hazard. If the fire hazard is not removed within the time allowed it shall be deemed a nuisance, and the Fire Chief or his deputy may have the same removed by the City, and the cost of such removal shall be recovered in an action by the City against the owner of the property and may also be entered on the tax roll as a special charge against the property.

F. Entering on premises. No person shall deny the Fire Inspector or his deputies free access to any property within the City at any reasonable time for the purpose of making fire inspections. No person shall hinder or obstruct the Fire Inspector in the performance of his duty or refuse to observe any lawful direction given by him.

Section 2: This ordinance shall take effect and be in force after its passage and publication in a manner provided for by law.

Acted on and adopted at a result meeting of the Common Council on July 17h, 2025.

CITY OF WATERLOO

_____
Jenifer Quimby, Mayor

Attest:

_____
Jeanne Ritter, City Clerk

Date Adopted:

Date Published:

136 North Monroe Street, Waterloo, Wisconsin 53594-1198
Phone (920) 478-3025
Fax (920) 478-2021

ORDINANCE #2025-10

AN ORDINANCE TO ADOPT THE ADMINISTRATIVE CODE of the DEPARTMENT OF SAFETY AND PROFESSIONAL SERVICES

The City Council of the City of Waterloo, Wisconsin does ordain as follows:

SECTION 1: § 200-2 **Adoption of Administrative Code provisions.**

A. The following chapters of the Wisconsin Administrative Code, Rules of the ~~Department of Commerce~~ Department of Safety and Professional Services, are hereby amended as follows:

~~COMM 2~~ SPS 302	Fee Schedule
~~COMM 7~~ SPS307	Explosives and Fireworks
~~COMM 10~~	~~Flammable and Combustible Liquids~~
~~COMM 14~~ SPS 314	Fire Prevention
~~COMM 32~~ SPS332	Public Employee Safety and Health
~~COMM 40~~ SPS340	Gas Systems
~~COMM 61 to 65~~ SPS 361-366	Commercial Building Code

B. ~~A copy of the above codes is on file in the office of the Fire Chief.~~ A copy of the above SPS code is available at https://dsps.wi.gov/Pages/Programs/AdministativeRules.aspx

NFPA 1 is on File in the Inspection Office

SECTION 2: This Ordinance shall take effect upon passage by a majority vote of the members-elect of the City Council and publication/posting as required by law.

Adopted at a regular meeting of the Common Council on July 17, 2025.

CITY OF WATERLOO

Signed: _____
Jenifer Quimby, Mayor

Attest: _____
Jeanne Ritter, Clerk/Deputy Treasurer

Date Adopted:

Date Published:

FINANCE AND PERSONNEL COMMITTEE

ROLLING TASK LIST

1. EMPLOYEE HANDBOOK – REFRESH
   *Vacation policy
   *Sick Leave – updated
   *Residency requirement

~~2. NEW HANDBOOK POLICY - ANTI-BULLYING~~ Approved - June 2025

3. NEW HANDBOOK POLICY – AI
   Committee of department heads - 1st meeting 7/8/25

4. FIRE CHIEF MEETING - ROLE AND EXPECTATIONS FOR POSITION
   a. Sale of Equipment; wants 3rd Ambulance & another Brush Truck

~~5. DPW/PARKS DEPT HEADS – PERSONNEL SUPERVISION PROCEDURES~~
   Approved in May (DPW) and June (Parks) 2025

6. WU DELINQUENT UTILITIES – MBHM/COLLECTION FEES & LEGAL FEES

7. FIRE DEPARTMENT – DONATIONS/ORDINANCE (3 accounts)

8. UTILITIES/CITY WRITE-OFF FROM AUDIT

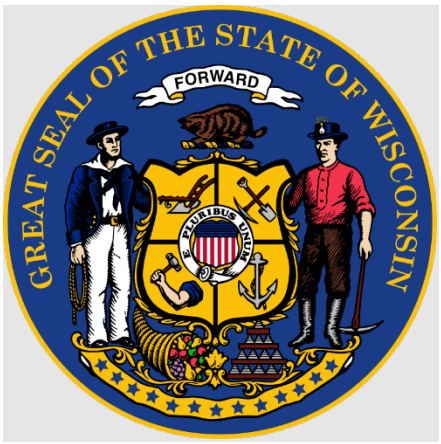
*Lana zeroed out, need to review issue and bill back Utility if needed (from 2019, 2022)

**In process of reconciliation of the account.

9. PLANS FOR HICKORY AND MAPLE ST – REVIEW-HOUSING

10. POLICY FOR ROADS AND SHARING COST WITH UTILITIES

* 33% has been prior practice, not written anywhere. Hendricks will be split as part of USDA information.



State of Wisconsin – Acceptable Technology Use, Access, and Security Policy

Effective Date: March 10, 2025

Information for Agency IT:

Legal Authority for, and Applicability of, Policy:

Pursuant to the legal authority and mandates set forth in Wis. Stat. §§ 16.971-16.975, the State of Wisconsin Department of Administration (DOA)'s Division of Enterprise Technology (DET), must, among other duties and responsibilities: 1) ensure that information technology (IT) services and resources are available to all executive branch agencies; 2) prescribe policies, standards, procedures, and safeguards for the security and privacy of the information and data contained within those State-managed IT Resources; and 3) ensure that all executive branch agencies develop and operate with clear guidelines. *See, e.g.,* Wis. Stat. § 16.971(2)(a); §§ 16.973(3), (4), and (5); § 16.974(3).

Accordingly, this enterprise-wide Acceptable Technology Use, Access, and Security Policy shall apply to all executive branch agencies, as defined by Wis. Stat. §§ 16.97(5m) and 16.70(4). This shall not apply to the following: Wisconsin Department of Justice, Wisconsin Department of Military Affairs, State of Wisconsin Investment Board, University of Wisconsin System Board of Regents, and the Wisconsin Technical College System Board.

Policy Exceptions:

With respect to the scope outlined in this policy, these are the minimum DET-established policies, standards, and procedures that all executive branch agencies are required to follow. Agency IT Directors are permitted to develop and implement policies, standards, procedures, or requirements for their users that are more stringent than are set forth in this enterprise policy. Agencies that do so should seek guidance and approval from agency legal counsel before developing and implementing those agency policies, standards, procedures, or requirements, to ensure compliance with any laws or standards applicable to the agency's work.

However, agencies are prohibited from developing or implementing policies, standards, procedures, or requirements that directly conflict with this enterprise policy without first requesting and receiving an exception from DET through established DET processes. Before making the request to DET for an exception, agencies are required to receive approval from their legal counsel to ensure the exception can be implemented consistently with the legal requirements applicable to an agency's work.

Questions regarding the risk exception procedures should be directed to the agency's IT Director (through the agency's service request [SR] process or other established IT processes), or to agency legal counsel.

Information for All Users:

Policy Statement:

The State of Wisconsin uses and manages a variety of IT Resources for its operations. Those State-managed IT Resources (as defined below) include, but are not limited to, information, data, equipment, systems, platforms, applications, and facilities. Users' usage of and access to these State-managed IT Resources has significant benefits for the State's operations and for users themselves (*e.g.,* remote/hybrid work), but also can create significant risks to the State, including IT security risks, as well as other legal, operational, audit, privacy, and financial risks.

Therefore, users' use of State-managed IT Resources comes with the expectation that these resources will be used in a manner consistent with stated policies, laws, and regulations. Using State-managed IT Resources in a manner inconsistent with this policy creates liability, security, privacy, and accountability risks which compromise the services that we provide to the public.

Questions about this policy can be directed to the user's supervisor, agency Human Resources, agency IT Director (through the agency's service request [SR] process or other established IT processes), or agency legal counsel.

Scope of Policy:

The responsibilities outlined in this policy apply to all users who are granted rights to access State-managed IT Resources, including all employees and all other non-employee users who are granted rights to use or access State-managed IT Resources through a contractual relationship or other relationship with the State.

A complete listing of authorized State-managed IT Resources, information, equipment, systems, platforms, applications, and facilities is not feasible or desirable, given that technology, data, and access across the State varies and technology rapidly evolves and changes. However, this policy outlines the authorized access and uses of, and applies to, all State-managed IT Resources used in conducting State business.

This Acceptable Technology Use, Access, and Security Policy primarily pertains to policies, standards, and procedures related to State-managed IT Resources, pursuant to DET's statutory authority. However, it also may include references to work rules,

laws/regulations, and other policies. This policy is not intended to supplant, supersede, or replace other policies; users must ensure that they abide by all relevant work rules, laws/regulations, and other policies that are stated elsewhere.

Definitions:

"*Appropriate Security Measures*" means reasonable technical, physical, and procedural controls to protect data against destruction, loss, alteration, unauthorized disclosure, and unauthorized access, whether by accident or otherwise, by employees or other authorized users including contractors. The State of Wisconsin IT Security Policy Handbook has been developed to provide a baseline of executive branch IT security policies and controls, and can be found here: DET Policies, Standards, and Procedures.

"*Artificial intelligence*" (or "AI") means any IT system or part of an IT system able to perform specific tasks that normally require human intelligence. A complete listing of all such technologies or capabilities is not feasible or desirable, but at present includes capabilities such as visual perception, speech recognition, decision-making, creation of new content, documentation and/or data, and language translation.

"*Authorization*" means the security process that an agency uses to determine a user's or service's level of access, as well as legal authority to access. Agencies have staff defined within their organization to determine the appropriate permissions, access privileges, and/or authorizations to access certain kinds of Non-Public Information (as defined below), or to perform particular actions. Users should direct all questions about authorizations, permissions, access privileges, and security processes to their supervisor, agency Human Resources, agency IT Director (through the agency's service request [SR] process), or agency legal counsel.

"*Enterprise Service Desk*" means the 24x7x365 IT support center providing users with a single point of contact for any Division of Enterprise Technology (DET)-managed or supported IT service.

"*Non-Public Information*" means any sensitive or confidential information whose use, dissemination, disclosure, or re-disclosure is protected, restricted, or prohibited from being disclosed by federal or state laws or regulations, or else should be treated confidentially or restricted pursuant to industry standards, policies, and procedures. Examples of "non-public information" include, but are not limited to, personally identifiable information ("PII"), protected health information ("PHI"), student

educational records or information, financial records or information, social security numbers, driver's license information, federal or state tax information, trade secrets, proprietary information, or attorney-client privileged information.

"*PHI*" or "*Protected Health Information*" has the meaning given in Wis. Stat. § 146.816(1)(f) and 45 C.F.R. § 160.103.

"*PII*" or "*Personally Identifiable Information*" has the meaning given in Wis. Stat. § 19.62(5). PII can also include information that, by itself, is not identifying, but when combined with other information could identify a specific individual.

"*Record*" has the meaning given in Wis. Stat. §§ 16.61(2)(b) and 19.32(2).

"*State*" means the State of Wisconsin.

"*State Credentials*" or "Security Credentials" means a proof of identity, such as passwords, biometrics, X.509, digital certificates, key cards, and USB tokens, which control access to information systems.

"*State-managed IT Resources*" include but are not limited to:

- Any State-provided or State-managed information technology device, which may include a computer, computer monitor, fax machine, copy machine, scanner, multi-function device, printer, camera, cellular telephone, tablet, mobile hotspot, or any other State-provided electronic or mobile device which can send, receive, display, or record data, text, pictures, video, or audio through any medium.

- Any State-provided or State-managed e-mail address or other similar State credentials used to access State-managed IT Resources, software, hardware, information system, cloud computing service, social media platforms, other services connected to or hosted on the State network, or other technology provided by the State to a user, or managed by the State, for work purposes.

- The use of voice or data connectivity through any State-provided or State-managed resource, which includes but is not limited to a wired network, wireless network, mobile hotspot, cellular telephone (including voicemail and other

similar Voice over IP [VoIP] systems), remote desktop or virtual desktop, virtual private network, or any other State-provided or State-managed service.

General Usage:

Users of State-managed IT Resources must abide by the following general provisions while using State-managed IT Resources:

- You shall not knowingly or intentionally use State-managed IT Resources to violate any federal, state, or local laws, regulations, or policies, including the State Employee Code of Ethics.

- You shall not use State-managed IT Resources in a manner inconsistent with the terms and conditions governing their use.

- You acknowledge that State-managed IT Resources are constantly monitored by the State for cybersecurity purposes.

- You acknowledge that you have no expectation of privacy associated with the use of State-managed IT Resources. Any information you send, receive, store, or view on State-managed IT Resources is subject to management review and may be monitored, including websites visited and personal communications, both during and outside of work hours.

- You acknowledge that State-managed IT Resources are the property of the State, including all communications sent or received on behalf of the State. As discussed below, all communications sent or received by users are presumed to be public records subject to release under the Wisconsin Public Records Law.

- You may only access data, documents, correspondence, and other records and information that you have been authorized to access and that are necessary to complete your work for the State of Wisconsin.
    - Access to data, documents, correspondence, and other records and information without authorization or for any other purpose is prohibited.

- You acknowledge that all State-managed IT Resources are subject to intellectual property laws, including patents, copyrights, trademarks, and trade secrets, and shall be used in accordance with relevant laws and regulations.
    - When using State-managed IT Resources with content that may be subject to intellectual property protection (*e.g.,* photos, graphics, recordings,

documents, and other information), you must ensure that you have the necessary permission from the owner to use it.

- You shall only communicate using State-managed IT Resources in a manner that is respectful and professional. Harassment, discriminatory conduct, hate speech, and other offensive behavior are prohibited while using State-managed IT Resources.
    - This also applies if you are using State-managed IT Resources to engage on social media, or if you are engaging on social media using a personal device or account in a way that could be attributed to the State of Wisconsin. *See* Wisconsin Human Resources Handbook Chapter 480 (Social Media Usage in State Government) and other applicable enterprise or agency social media policies.

- You are prohibited from using State-managed IT Resources to download, view, solicit, seek, display, or distribute any obscene, pornographic, offensive, or excessively violent material, unless specifically authorized to perform your work responsibilities for the State of Wisconsin.

Regarding Non-Public Information:

Users of State-managed IT Resources acknowledge that the information, data, and knowledge made available for State-related business purposes must be kept safe, and Non-Public Information must be treated as confidential or sensitive. This is necessary to preserve the integrity of State of Wisconsin operations and services.

- You are prohibited from using, disclosing, communicating, or transmitting Non-Public Information without proper authorization, including but not limited to:
    - Copying or transferring Non-Public Information to any form of removable media (*e.g.,* external hard drives, flash drives) without proper authorization.
    - Revealing Non-Public Information on newsgroups, forums, mailing lists, websites, chat rooms, or other similar public/semi-public forums.
    - Accessing or disclosing Non-Public information for any purpose not related to State business, or for any other non-authorized purpose.

- You shall utilize appropriate security measures for all authorized uses, disclosures, communications, transmissions, copies, or transfers of Non-Public Information.
    - You shall immediately contact your agency IT help desk or the Enterprise Service Desk, as soon as you become aware of any suspected or actual unauthorized use, disclosure, communication, transmission, copy, or transfer of Non-Public Information, including the loss or theft of removable media (*e.g.,* external hard drives, flash drives) which may contain Non-Public Information.
    - You must provide this notification even if the unauthorized use or disclosure was inadvertent or accidental. This will allow the agency to determine whether it needs to initiate any legally required mitigation or notification actions, pursuant to each agency's incident response plan. *See* DET's Standard 170 Incident Response Standard.

- You acknowledge that shared files, groups of files, or folders must have proper security configurations, encryptions, and permissions/access rights to comply with legal and regulatory requirements related to Non-Public Information.

- You should avoid disclosing Non-Public Information over text and other non-encrypted or non-secure messaging platforms. Doing so not only creates public records that must be retained and produced, if requested, but may also create unnecessary security and privacy risks.

Public Records and Records Retention:

A comprehensive description of users' public records and records retention obligations is outside the scope of this policy. However, users should assume that any records and other electronic content on State-managed IT Resources (*and* content on personal devices) that are created or being kept in connection with the official purpose or function of the agency are "records" that: 1) should be evaluated by the agency's legal counsel before disclosure to the public, pursuant to the agency's normal public records request processes; and 2) should be retained for the time periods set forth in the applicable General Records Retention Schedule (GRS) or agency-specific Records Retention/Disposition Authorization (RDA).

Users should follow these general records guidelines, in addition to any agency-specific policies or guidelines, to assist in ensuring compliance with public records and

records retention responsibilities and obligations while using State-managed IT Resources:

- The definition of "record" includes but is not limited to electronic records (*e.g.,* emails, Teams chats, text messages), content on virtual platforms (both during meetings and outside of meetings), data, social media content, voicemails, and audio/video recordings, generative AI output, etc., that are created or being kept in connection with State business.
    - If you are using State-managed IT Resources to engage on social media, or if you are engaging on social media using a *personal* device or *personal* account in a way that could be attributed to the State of Wisconsin, you must abide by Wisconsin Human Resources Handbook Chapter 480 (Social Media Usage in State Government) and other applicable enterprise or agency social media policies.

- In addition to applicable records retention schedules, other laws and circumstances may require some records to be retained for longer, such as when a public records request has been made for a record, or if the record pertains to a complaint, investigation, or ongoing litigation.
    - Those retention timeframes may extend beyond the user's period of employment or contractual or other connection with the State.
    - Therefore, before deleting any records, users should consult their supervisor, agency legal counsel, or agency records officer.

Questions about these affirmative records responsibilities, duties, and obligations can be directed to the user's supervisor, agency records officer, or agency legal counsel.

Use of Personal Devices and Personal Accounts:

Users should also follow these general guidelines, in addition to any agency-specific guidelines, to assist in ensuring compliance with public records and records retention responsibilities and obligations:

- You acknowledge that all work-related records (including but not limited to data, communications, pictures, audio, video, or other information) housed on personal *devices* and on personal *accounts* are considered records and are subject to disclosure under the Wisconsin Public Records Law. Such records must also be retained, maintained, and safeguarded per relevant records retention schedules.

- You are encouraged to always use State-managed IT Resources, including State email, Teams, and text messaging on State-issued mobile devices to conduct State business. Doing so will help ensure proper records retention on State-managed IT systems and help protect State-managed IT Resources, information, and data through proper security practices.

- The use of personal *accounts* (*e.g.,* Gmail for emails, personal text messaging *accounts*, and other similar instant messaging-type *accounts* like WhatsApp, etc.) for State business is strongly discouraged. You should not use personal *accounts* to conduct State business, except in very limited circumstances where it is not possible to use State-managed IT Resources.
  - If you use a personal account to conduct State business and create any records using that personal account, you are responsible both for the proper retention of such records, and for making such records available if requested by the public, as well as compliance with any other legal requirements and enterprise or agency policies applicable to the records.
  - With respect to certain types of Non-Public Information (*e.g.,* PII, PHI), the use of personal accounts may also violate other aspects of this policy, other applicable laws or regulations, or enterprise or agency policies. In most instances, users should not use personal accounts to transmit or store Non-Public Information.

- When using personal *devices* or personal *accounts* to conduct State business, you must also ensure that all other security and usage requirements are being met. This includes but is not limited to:
  - Logging into State accounts using State Credentials.
  - Utilizing a secure VPN connection to access State-managed IT Resources when not connected to a State network (*e.g.,* when not connected by state ethernet or Wi-Fi, but when using public or non-secure Wi-Fi).
  - Enabling multi-factor authentication to access Non-Public Information on non-State-issued devices or non-State-managed IT Resources.
  - Not conducting any State business on personal devices or personal accounts using prohibited vendors and technologies, pursuant to DET Standard 290 Removal of Prohibited Foreign Products Standard.
  - Ensuring that any other agency or enterprise policies are followed when using personal devices (*e.g.,* agency Bring Your Own Device policies).

Transcriptions and Recordings:

Information for Agency IT:

Regarding transcriptions and recordings, a comprehensive enterprise-wide policy is neither feasible nor desirable. Each State-managed IT Resource may have its own functionality regarding whether a transcription and/or recording can be made from audio, video, or both (*e.g.,* virtual meetings). Each agency may also have its own needs, policies, and legal requirements regarding permissible uses of transcription and recording functionality. Some transcription and recording functionality may also be enabled by default. Moreover, some State-managed IT Resources may require transcriptions or recordings to be enabled in order to access AI-enabled functionality (*e.g.,* meeting summaries), including AI-enabled functionality that is not yet widely available or not yet in use enterprise-wide. Therefore, agencies are responsible for creating their own policies regarding transcriptions and recordings, and must abide by all relevant DET policies, standards, and procedures if transcription/recording functionality is enabled.

Agency policies must follow all applicable laws, regulations, standards, and procedures to ensure that such recordings or transmissions are not prohibited by law, do not contain Non-Public Information, and do not use Non-Public Information to train a large language model (LLM) contained within AI-enabled technology.

Information for Users:

When deciding whether to transcribe or record a meeting or conversation, users should follow these general guidelines, in addition to any agency-specific guidelines, to assist in ensuring compliance with any applicable laws, regulations, policies, and other requirements related to transcriptions and recordings:

- Unless there is an agency policy expressly permitting such recordings or transcriptions, *and* a business need to record/transcribe, you are strongly discouraged from recording or transcribing any conversations or meetings that occur in audio or video messaging applications, including but not limited to Teams and audio recorders on electronic devices.
    - Transcriptions often contain errors and may not accurately reflect the communication made by the caller or the meeting participant(s).
    - Video and audio recordings are also expensive to retain.

- Before recording or transcribing a meeting or conversation, you must obtain authorization from your supervisor, and you must also notify all attendees or participants that the meeting or conversation is being recorded or transcribed.

- If you have received authorization to record or transcribe meetings, and if such transcriptions or recordings are permissible by agency policy, you must retain the audio/video recording and/or the transcription securely for the relevant records retention period mandated by law.
    - Transcriptions and recordings are distinct records, and both must be retained under relevant records retention periods.
    - Other records created from a transcription and/or recording (*e.g.,* meeting minutes, interview summaries) are also records, and distinct from the transcription/recording. Both should be retained under relevant records retention periods.
    - Transcriptions and recordings are subject to disclosure under the public records law and may be released to the public, if requested.

Users should direct any questions about transcriptions and recordings to their supervisor, agency IT Director, or agency legal counsel.

Closed Captioning:

This transcription/recording policy does not apply to live closed captioning, which may be enabled by anyone during a meeting or call and does not create a record. If a user needs to record or transcribe a meeting as a reasonable accommodation for a disability-related need, please contact your agency's medical coordinator to obtain that accommodation.

IT Security:

The security and safety of State-managed IT Resources is of the utmost importance. In addition to any agency security standards, all users must comply with the following security standards, processes, and practices:

- You should keep all usernames, passwords, multi-factor authentication codes, and other information used to access State-managed IT Resources confidential and never share with others.

    - State of Wisconsin agency IT help desk and Enterprise Service Desk staff will never ask for a user's passwords or codes.
    - If you believe your passwords or codes have been compromised, you should immediately contact your agency IT help desk or the Enterprise Service Desk.

- You shall not use any software, tools, or services that permits another user to remotely access or control another system on any State-managed IT Resource without authorization from your supervisor.
    - This prohibition does not apply to authorized remote access by DET or agency IT personnel for authorized purposes (*e.g.,* help desk).

- You shall not reroute traffic on, scan, probe, or attack a network without authorization.

- You shall not intercept or attempt to intercept any data or other information without authorization.

- You shall not use unauthorized peer-to-peer (P2P) networking, file sharing, instant messaging, or Internet Relay Chat (IRC) applications or services.

- You shall not install or attach any equipment to State-managed IT Resource without your agency's authorization (*e.g.,* wireless access points, modems, disk drives, external hard drives, networking devices, personal mobile devices or computers, monitors, keyboards, mice, printers, etc.). Any unauthorized equipment may be confiscated.
    - This applies to equipment being used, installed, or attached anywhere (*e.g.,* in the office, at home, at remote work location sites, in the community, etc.).
    - For additional information about equipment being used for remote work, *see* Wisconsin Human Resources Handbook, Chapter 748 Remote Work and any applicable agency remote work policies.

- You shall not intentionally modify, damage, repurpose for personal use, or remove State-managed IT Resources without authorization.

- You shall not modify, disable, test, or circumvent any State-managed IT Resource security controls, safeguards, or access controls without authorization.

- You shall not intentionally cause a security incident resulting in a loss of data confidentiality or integrity, or a disruption or denial of availability.
    - This includes using State-managed IT Resources to obtain, or to attempt to obtain, unauthorized access to another computer, to make unauthorized modifications to data, computer programs or supporting documentation, to improperly disrupt the operation of another computer, or to commit any crime.

- You shall not circumvent user authentication or compromise the security of a host, network, or account.

- You shall not compromise, modify, or cause damage to State-managed IT Resources.

- You shall not disrupt or interfere with the normal operation of any State-managed IT Resource.

- You shall not download, install, configure, or modify software or hardware without authorization.

- You shall not store data, records, or other information in public storage services or removable devices, without authorization.

- You shall not use or share any program, disk image, archive, or any form of executable files without authorization.

Suspected Unauthorized Use/Security Incidents:

Users must stop using a State-managed IT Resource when they become aware that it may have been involved in a suspected or actual security incident, data breach, or unauthorized use or disclosure.

- You must use alternative communication methods to report the suspected incident, pursuant to each agency's incident response plan. *See* DET's Standard 170 Incident Response Standard.

- Wait for further instructions prior to doing anything further with the State-managed IT Resource.

- You must not delete anything related to such suspected security incident, data breach, or unauthorized use/disclosure, as such information may legally be required to be kept and/or may assist in a later investigation.

State Credentials/Security Credentials:

Users must take precautions to not disclose information related to State Credentials or Security Credentials. As noted above, users should keep all usernames, passwords, multi-factor authentication codes, and other information used to access State-managed IT Resources confidential and never share with others.

In addition, to prevent information and security compromises, users must adhere to the following:

- Do not provide your State of Wisconsin issued email address, or the email address of other State of Wisconsin employees or contractors, to others on a public forum or while using artificial intelligence (AI) tools without authorization to do so as a State of Wisconsin representative.
  - If you are using State-managed IT Resources to engage in a public forum (including but not limited to social media), or if you are engaging in a public forum using a *personal* device in a way that could be attributed to the State of Wisconsin (including but not limited to using your State of Wisconsin issued email address), you must abide by Wisconsin Human Resources Handbook Chapter 480 (Social Media Usage in State Government) and other applicable enterprise or agency social media policies.
  - If you are using State-managed IT Resources while using artificial intelligence (AI) tools (including but not limited to generative AI tools), or if you are using AI tools using a *personal* device in a way that could be attributed to the State of Wisconsin, you must abide by the requirements for use of AI as stated elsewhere in this policy, along with any other applicable enterprise or agency AI policies.

- Do not re-use passwords from State-managed IT Resources for use on any non-State-managed IT Resources.

- Do not reveal or allow anyone to know or use your State Credentials.

- Do not access State-managed IT Resources with Administrator Credentials or administrator authority unless authorized. If administrator authority is necessary to run an application or perform a task, only approved agency processes may be used to grant that administrator authority.

Workstation/Device Usage:

Users of State-managed IT Resources are expected to keep State-managed IT Resources safe and take all necessary steps to ensure protection from unauthorized use or unauthorized modification, and to ensure that those State-managed IT Resources are maintained within authorized and secure locations.

These State-managed IT Resources are supplied to assist users in providing State services, and as such, must be used and maintained according to this policy and other relevant state and federal laws, policies, regulations, and guidelines. Users must take the following precautions to protect State-managed IT Resources:

- You must lock or log off State-managed IT Resources when unattended.

- Do not use State-managed IT Resources or access State data outside the boundaries of the United States.
    - Use of State-managed IT Resources and access of State data outside the United States is strictly prohibited, except in very limited circumstances and in accordance with DET's International Travel Procedures.
    - International use of State-managed IT resources causes an unacceptable level of cybersecurity risk that in many cases cannot be mitigated.
    - Any use case exceptions for international use must be submitted through DET's risk exception process and pre-approved by both the agency IT director and the agency head before users use State-managed IT Resources outside of United States.
    - This prohibition also includes all State-provided or State-managed IT Resources housed on personal devices (*e.g.,* applications including but not limited to Teams and Outlook).

- Do not bypass or circumvent VPN, firewall, antivirus, or other security measures.

- Non-State Wi-Fi access is inherently not secure, and you should use appropriate security measures when using any State-managed IT Resources that are not connected to a State system or network (*e.g.,* when not connected by state ethernet or Wi-Fi, when using public or non-secure Wi-Fi). Those security measures include but are not limited to:
    - Logging into State accounts using State-provided Credentials.
    - Utilizing a secure VPN connection to access State-managed IT Resources.

- Only devices authorized by your agency may be attached, plugged into, connected with, docked with, paired to, or otherwise provided access to State-managed IT Resources.
    - This includes external hard drives, USB flash drives, memory cards, Bluetooth devices, RFID devices, NFC devices, docks, monitors, keyboards, and mice.

- Removing any State-managed IT Resource other than a State-provided devices, including but not limited to laptops, headsets, webcams, cellular telephone, mobile hotspot, payment processing equipment, or tablet from a user's workspace, including a home office, is prohibited without proper authorization.

- You are responsible for all State-managed IT Resources that have been assigned access and/or issued to you. Damage, loss, or theft of State-issued or State-managed equipment should be immediately reported to your agency IT help desk or the Enterprise Service Desk.

- Repairs to State-issued or State-managed equipment shall be completed only by authorized agency employees, vendors, or contractors.

Personal Use of State-managed IT Resources:

Users of State-managed IT Resources must protect those resources from unauthorized access and misuse. Access is given to assist you in providing State services and to perform State business. To accomplish this, any State-managed IT Resources must only be used in support of approved and authorized State business activities and must not be put at risk by unauthorized access or activity.

Regarding any personal use of State-managed IT Resources, users must abide by the following provisions:

- Do not use State-managed IT Resources for any political or commercial purpose.
    - "Political purpose" is defined in DPM Bulletin DPM-0580-MRS.
    - "Commercial purpose" is defined as any activity for which an employee receives payment or compensation other than through their employment or other contractual relationship with the State of Wisconsin.

- Consistent with State of Wisconsin work rules, you are at all times prohibited from using State-managed IT Resources for engaging in unauthorized activities, including but not limited to gambling, operating a personal business, soliciting, playing games, or any other conduct that is disruptive, decreases the user's productivity, or increases agency costs.

- You acknowledge that any personal use of State-managed IT Resources should be incidental or minimal, including storage of non-work-related files or data on State-managed IT Resources.
    - If you download or store non-work-related files or data on State-managed IT Resources, you must ensure that doing so does not create a security or data privacy risk.
    - It is also recommended that you label any personal files or data housed on State-managed IT Resources, and/or place personal files or data in clearly marked personal folders, especially on shared network drives.

- If using State-managed IT Resources for incidental personal use, you shall not disrupt or interfere with the normal operation of any State-managed IT Resource, including but not limited to causing unnecessary network congestion or application delays within State-managed IT Resources (*e.g.,* streaming video or audio during work hours).

Network Usage:

- Do not bypass or circumvent any State of Wisconsin cybersecurity measure or disrupt the operation of any computer or information system.

- Do not connect any non-State-managed device to a State-managed network unless authorized.

- Do not attempt to bypass State-managed firewalls, routers, or other security systems.

- Do not attempt to access any State-managed IT Resource that you have not been given access to or have not been authorized.

- Do not share any network information such as IP addresses, Wi-Fi passwords, jack location, or other details with anyone unless explicitly requested by approved agency support personnel.

Artificial Intelligence (AI) Usage:

Information for Agency IT:

The State of Wisconsin may seek to use Artificial Intelligence (AI) platforms to leverage their capabilities in gaining unique insights, problem solving, and enhancing productivity at state agencies. It is important to note that each agency and each State-managed IT Resource may have access to its own AI functionality, and needs, policies, and legal requirements regarding its permissible uses of AI technology. AI technology is evolving and developing rapidly; at this time, it is not possible to anticipate all possible uses of AI technology, or risks of those uses.

Therefore, until such time when enterprise frameworks, policies, standards, and procedures are in place, agencies are responsible for creating their own AI policies regarding evaluation and use of AI technology within their agency. Agency AI policies must be reviewed and approved by DOA. Such policies must be consistent with all relevant DET policies, standards, and procedures where AI functionality is enabled or used within State-managed IT Resources. DOA may require agencies to submit additional information, including information from agency legal counsel, as part of the approval process. Once approved, an agency may implement the AI policy to approve AI functionality for purchase and/or use by employees.

Information for Users:

Safeguarding sensitive or confidential information from unauthorized access, use, or disclosure is of utmost importance. Before using AI technology, particularly open-source or publicly available generative AI technology (*e.g.,* Chat GPT, Gemini, etc.), users should review their agency AI policy for any agency-specific requirements. This will help ensure that AI platforms and any associated data handling processes complies with applicable confidentiality and data protection laws and regulations, contractual or legal

obligations. This will also help ensure that the use of AI platforms aligns with existing agency, DET, and enterprise policies that concern but are not limited to data privacy, confidentiality, security, and intellectual property protection. At minimum, users must follow these general guidelines to assist in ensuring safe use of AI and proper compliance:

- You must only use AI platforms and functions that have been authorized for use at your agency and that you have received authorization to use for a specific use case or business purpose.

- You should familiarize yourself and comply with any applicable agency policies, all terms and conditions of the AI platform itself, and any other laws and regulations, including public records and records retention laws.

- You are prohibited from using State Credentials when engaging with AI technology in a personal capacity or on a personal device, unless you have received prior authorization to do so. However, when using an authorized AI tool on State-managed IT resources, you should use your State Credentials to engage with the AI tool.

- You are strictly prohibited from sharing Non-Public Information with any internal or external generative AI platform that has not been authorized for use at your agency.
    - You should be vigilant in using generative AI tools and should report to your supervisor or IT staff the appearance of, or others' unauthorized use of, Non-Public Information in generative AI input or output.
    - You should take care to avoid including specific project details, proprietary information, internal jargon, or any other information that could potentially compromise confidentiality, privacy, or data security, or infringe upon the State's or others' intellectual property rights.

- As a user of State-managed IT Resources, you are responsible for using any AI tools ethically, transparently, and in a manner that minimizes bias and discrimination.
    - Given the known risk of factual errors and algorithmic bias in AI-generated output, you must exercise critical judgment and verify the completeness and accuracy of all information from any AI platform, especially generative AI.

        - You should report to your supervisor or IT staff any erratic or inaccurate behavior of the authorized AI tool.
    - You are prohibited from using AI tools in a way that would violate State of Wisconsin work rules, laws/regulations, and other policies that are stated elsewhere. This includes a prohibition creating or distributing content that is defamatory, discriminatory, malicious, deceptive, or infringes on the rights of others. Any such misuses of AI tools may result in termination of access or disciplinary action.
    - All uses of generative AI and predictive AI must be guided by “human-in-the-loop" principles to ensure that critical thinking and good judgment is exercised. Therefore, you must not deploy an AI output in your work on behalf of the State without conducting an appropriate level of review of such output. For example:
        - If authorized by your agency to create content using generative AI, (e.g., letter or email or memo), you must not use such content without first reviewing and revising it for accuracy, usefulness, and appropriateness of tone and substance;
        - You must not use a generative AI tool to assist with research without conducting independent checks of the content created for accuracy;
        - You must not instruct nor prompt generative AI tools or models to create content in the style of others, and you should clearly attribute any output solely created by AI for State business through a footnote or other means visible to the reader; and
        - Unless using an AI tool expressly authorized by your agency for an expressly authorized purpose, you must not solely use predictive AI for decision-making without also reviewing those predictions, decisions, or outputs, and exercising critical judgment about those predictions, decisions, or outputs.
    - Permissible uses of generative AI may include such uses as brainstorming or generating ideas. If a use case is not included in your agency’s AI policy, or if you are unsure whether a use is permissible, you should ask your supervisor before proceeding.

Internet Usage:

The internet enables users to access and leverage non-State-managed IT Resources, systems, and services, including cloud services. Users of these services must

be cautious and ensure that State security policies are not violated. You must also take the following precautions to protect State interests:

- State agencies have blocked many internet sites that are not appropriate for work purposes.
    - However, you should not assume that a website is appropriate simply because it is not blocked. Certain un-blocked internet sites may also be inappropriate for work purposes or prohibited by other policies.
    - You must abide by all other policies, work rules, and laws related to appropriate internet use.

- Do not use internet services for purposes other than those needed in support of your work duties, with limited, incidental personal use exceptions as outlined by this policy or related agency or enterprise policies.

- Do not share, exchange, transfer, reveal, or otherwise distribute data contained on State-managed IT Resources with any internet site without proper authorization.

- Do not import or download data or information from any internet sources directly into State-managed IT Resources without proper authorization.

- Do not copy, repost, or share information from internet sources unless the source is known, reliable, trustworthy, legal, accurate, public (*i.e.,* not Non-Public Information, sensitive, restricted, or otherwise protected), and properly credited or attributed to the original source.
    - You must also abide by all relevant intellectual property laws when copying, reposting, or sharing information.

Remote Work:

Users of State-managed IT Resources and technology may be allowed or required to work remotely (outside of a State-managed facility). Remote work has many advantages but also creates a unique set of risks and obligations that must be managed to ensure that State-managed systems and data are protected.

Users must abide by all the provisions of this Acceptable Use Policy described herein, as well as applicable human resources policies about remote work, *see*

Wisconsin Human Resources Handbook, Chapter 748 Remote Work and any applicable agency policies.

In addition, users must also take all the following precautions to protect State-managed IT Resources while engaging in remote work:

- The State will provide a computer for employees working from home and may provide other State-managed IT Resources and equipment at its discretion, but you must provision, configure, support, patch, and maintain any personal equipment and services that are needed to enable your remote work.
    - The State will only provide technical support for State-managed IT Resources and will not provide technical support for personal IT equipment and services.
- You must take appropriate steps to secure all State-managed IT Resources and work to prevent unauthorized access or unauthorized use:
    - You shall secure physical documents, lock screens when not in use, and use encryption or password protection for digital files and communications, as required by enterprise or agency policies.
    - You shall not share State-managed IT Resources with unauthorized individuals.
    - You shall not share or disclose Non-Public Information with unauthorized individuals.

Policy Violations:

Users must follow all relevant agency IT policies and procedures, in addition to this enterprise policy. All users must also understand and accept that violating any of these policies exposes the State of Wisconsin to unnecessary risk.

Accordingly, all users must acknowledge that violating any of these policies can constitute work rule violations. The potential consequences for violations include:

- Disciplinary actions, which can include warnings, suspension, or termination of employment, depending upon the severity and frequency of the behavior or violation of work rule.
- Criminal prosecution, if the behavior constitutes a criminal offense.
- Civil liability for behaviors outside the scope of employment.
- Restricted access or termination of access to State-managed IT Resources for users who violate this policy or pose a risk to the security, privacy, and integrity of State systems, networks, or data.

KENOSHA PUBLIC LIBRARY

Artificial Intelligence & Machine Learning Usage Policy

The Board of Trustees of the Kenosha Public Library adopts and makes public the following written policies.

Introduction & Objective

The Kenosha Public Library recognizes the potential of Generative Artificial Intelligence (GenAI, often referred to as AI) and Machine Learning (ML) to enhance workflows and productivity. However, the Library also acknowledges that irresponsible use of AI and ML can lead to significant issues. Therefore, the Kenosha Public Library is committed to using AI in a responsible and ethical manner. This policy establishes best practices for utilizing AI tools within the Library, with a particular focus on safeguarding sensitive data and patron information.

Definitions

Artificial Intelligence (AI)

AI refers to a broad field of computer science focused on creating intelligent systems that can perform tasks typically requiring human intelligence. AI is not a single technology, but rather a collection of methods and approaches aimed at achieving intelligent behavior in machines.[1]

Machine Learning (ML)

ML is a subfield of AI that focuses on creating algorithms that can learn from data without being explicitly programmed. These algorithms can analyze large amounts of data to identify patterns and trends, and then use that knowledge to make predictions or decisions on new data.[1]

Generative AI (GenAI)

GenAI is a type of AI that uses machine learning to create entirely new data, such as images, text, or audio. GenAI systems are trained on massive datasets and learn to identify the underlying patterns within that data to generate new content.[1]

AI Systems & Tools

An AI system, or tool, is a computer program designed to intelligently perform tasks. They receive various inputs, like data or user requests, and analyze them to achieve a specific goal, set by humans either directly or indirectly. AI systems can operate independently to varying

[1] Harris 2023

degrees, and some may even improve their performance over time without needing reprogramming.[2]

AI Hallucinations

GenAI systems are susceptible to producing outputs that deviate from intended results. These deviations, known as AI Hallucinations, can manifest as inaccurate, misleading, or entirely fabricated content.[2] Due to the potential for realistic and convincing hallucinations, critical evaluation of all GenAI outputs is essential.

Security

Prior to using any AI tool, employees must coordinate with Computer & Network Services (CNS) to conduct a thorough evaluation of its security practices. Tools must follow the Library's current Data Privacy & Security Guidelines and the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF) will be used to conduct a risk assessment of the AI tool.[3] To understand the steps involved in AI vetting, staff are encouraged to review the AI Vetting Process.

Data Protection

The Library prioritizes data security and patron privacy by strictly prohibiting the upload of confidential data (patron information, employee records, etc.) to unvetted AI systems. Uploading confidential or sensitive data is only permitted on vetted AI systems when the data is necessary for the system's functionality and falls within the scope of its intended use. Library staff may request the acquisition of an AI system for assisting their work within a specific scope. The requester will define the scope in the AI Vetting Request form.

The Head of IT, the AI Requestor, and an IT Staff member or Digital Strategy Librarian are responsible for vetting the AI system using the AI Vetting Process. The vetting process will identify mitigation strategies to prevent the exposure of sensitive and confidential data. These strategies may include restricting use within a vetted system and recommending a different system.

Sharing login credentials, confidential or sensitive data in such a way that third-party AI providers can view, use, sell, access, manipulate, train AI or related systems, or permanently store data, violates state law[4], KPL's Confidentiality Policy, and Library Bill of Rights Article VII. To protect patron privacy, KPL will do all within its power to disable desktop AI tools that passively monitor patron or staff behavior (See Appendix D for details on AI usage on Patron Computer).

[2] European Union 2024
[3] National Institute of Standards and Technology 2024
[4] Wisconsin State Legislature 1981

Transparency

Employees are expected to utilize AI and ML tools with integrity, honesty, and respect for individual rights and privacy. This includes proper attribution of AI-generated work and proper vetting of the AI tool's output, and ensuring that data used in ML algorithms is within the intended and vetted use of the AI tool

Original Works

When AI is used to assist in the creation of original works such as blogs, social media posts, reports, summaries, or marketing materials, acknowledgement of the role AI plays in the creation process is required. All original work in which AI plays a role in its creation will link to a statement (See Appendix B) indicating the use of AI. While AI may be used for various tasks, the Library will not employ text to image AI tools for the generation of original images or the generation of elements of the image.

Corrections and Inspiration

No attribution statement is required for using AI solely to correct spelling or grammar in original works or for generating inspiration for original creations. Examples of AI generated inspiration include:

- Brainstorming;
- Generation of ideas or examples that are further developed and refined;
- Aiding in research on a topic as a starting point; and
- The utilization of AI-generated images as individual components within a larger original work, with the option for further editing of these elements.

Responsible Use

AI and ML tools are for authorized business purposes only and must comply with all applicable laws, regulations, and Library policies. Employees must disclose AI generated answers in reference interactions.

Staff will cross-reference any answers generated by AI tools. A cross-reference may involve suggesting reliable sources for verification, such as academic journals or government websites. It is the expectation of all library staff to critically evaluate the source and potential for bias or errors in all information used, including AI tools (See Appendix C for AI Literacy).

AI will not be used to deceive, manipulate, mislead, misrepresent or otherwise falsify information in any conceivable manner.

Disclosure of AI & ML Tools used by KPL

The Kenosha Public Library will maintain a list of approved AI & ML tools and resources for staff use on the Privacy Information section of the website. This list will be updated as tools are added and include the following information for each tool:

- Name;
- Date added; and
- Description of how the product is used.

AI usage for Reference

Library Staff may use approved AI tools to enhance information searches. Staff will disclose AI use verbally and mark interactions on Patron Question forms. Staff will offer to guide patrons on source evaluation for credibility. For larger research topics, staff will cross-reference AI-generated answers with reliable sources such as academic journals or government websites.

ML Training Data

KPL prioritizes privacy in its ML datasets by minimizing data collection and removing sensitive attributes. Data will undergo anonymization before analysis, including removal of personally identifiable information and other protected data points[5]. Anonymization techniques such as hashing, k-anonymity, and differential privacy may be employed for further protection.

Mitigating Bias

Due to the potential for integrated bias, AI tools will not be used for selecting or narrowing down potential hiring candidates, or for disciplinary actions. The Library will prioritize human-centered approaches that ensure fairness and inclusivity.

Library staff utilizing AI and ML tools must review all output before publishing or using any generated materials.

Disciplinary Measures

Violations of this policy will be investigated and may result in disciplinary action, up to and including termination of employment. The severity of the disciplinary action will be determined based on the nature and severity of the violation.

Review and Updates

To ensure this policy remains effective in promoting the use of AI technology while safeguarding privacy, confidentiality, and compliance with the latest State and Federal Government

[5] Wisconsin State Legislature 1981

guidelines, it will be reviewed regularly, at least every six (6) months, or sooner if necessary. The Library reserves the right to update this policy to reflect the evolving regulatory landscape.

Appendix A: Information Sources

Department of Workforce Development. 2024. “Draft Action Plan.” Governor’s Task Force on Workforce and Artificial Intelligence. https://dwd.wisconsin.gov/ai-taskforce/meetings/pdf/240503-draft-action-plan.pdf.

European Union. 2024. “EU Artificial Intelligence Act.” The AI Act Explorer. https://artificialintelligenceact.eu/ai-act-explorer/.

Harris, Laurie. 2023. “Congressional Research Service.” Generative Artificial Intelligence: Overview, Issues, And ... https://crsreports.congress.gov/product/pdf/IF/IF12426/1.

National Institute of Standards and Technology. 2024. “Ai Risk Management Framework.” Ai Risk Management Framework. https://www.nist.gov/itl/ai-risk-management-framework.

Wisconsin State Legislature. 1981. “Public Library Records.” Wisconsin Legislature: 43.30.

https://docs.legis.wisconsin.gov/statutes/statutes/43/30.

Appendix B: Statement on AI Usage

Kenosha Public Library is committed to embracing innovation. This includes using Artificial Intelligence (AI) to enhance patron experiences while doing diligent work to protect patron privacy.

In order to maintain transparency, Kenosha Public Library will link to this statement whenever AI plays a significant role in content creation. All AI tools Kenosha Public Library uses are thoroughly reviewed for privacy and all content created is vetted by staff members for accuracy and consistency.

Appendix C: AI Literacy

The Kenosha Public Library is committed to promoting digital literacy and information fluency. AI literacy includes the knowledge and skills that enables community members and staff to critically understand, use, and evaluate AI systems and tools to safely and ethically participate in its influence on the digital world.

The Library will coordinate with local educational institutions to coordinate educational efforts and share best practices on AI literacy.[6]

Patron Education

The Library's AI Literacy targets include but are not limited to:

- Knowledge of the data and methods that were used to train this AI system or tool;[6]
- Perception of data privacy, security while using AI tools;
- Understanding of copyright and fair use in regards to AI tools;[7]
- Consideration of how datasets, including their accessibility and representation, reproduce bias in society;
- Examination of the credibility of outputs, the efficacy of algorithm, and questioning the biases inherent in the use of AI systems and tools; and
- Distinguishing between human made and AI generated works.

Staff Training

To ensure a comprehensive understanding of AI and its impact on library operations, staff training will be tailored to different position groups. This will allow staff to develop a deeper knowledge relevant to their specific roles and responsibilities within the library.

In addition to receiving training on the same topics as patrons, staff will also be provided training to give them a greater understanding of AI including:

- The history of AI & current day to day usage
- General Information Literacy to aid in answering patron questions
- The Library AI System vetting process
- A more in depth understanding of biases & hallucinations

[6] Department of Workforce Development 2024
[7] European Union 2024

Appendix D: Statement on AI usage on Patron Computers

Patrons may encounter various Artificial Intelligence (AI) products while using Kenosha Public Library computers. This could include AI-powered search engines, chatbots on websites and desktops, or recommendation algorithms. While AI can be a helpful tool, it's important to critically evaluate the information it provides. Here are some things to keep in mind:

- AI products are still under development and may not always provide accurate or unbiased information.
- It's important to assess the credibility of the source behind the AI product.
- Be mindful of potential biases in the information presented.

Unless otherwise stated, any AI applications that appear on Library computers are not endorsed by Kenosha Public Library. The Library will do all within its power to restrict desktop AI applications from accessing patron data that the patron has not voluntarily provided or enabled; this will include disabling such applications when possible.

Appendix E: Change Log

Date	Section Name	Change Description
05/29/2024	Full Document	Initial Draft

City of Waterloo, Wisconsin

Artificial Intelligence (AI) Governance & Acceptable Use Policy (DRAFT)

Adopted: [Insert Date]

1. Purpose

This policy establishes official guidelines for the acceptable use, governance, and oversight of Artificial Intelligence (AI) technologies by the City of Waterloo. It ensures that the use of AI in municipal operations is responsible, transparent, and aligned with the values of public trust, privacy, and service integrity.

2. Scope

This policy applies to all employees, elected officials, contractors, and volunteers who access, use, or manage AI technologies as part of any City of Waterloo operations, services, or communications.

3. Definitions

- Artificial Intelligence (AI): Any system or technology that performs tasks typically requiring human intelligence, including but not limited to natural language processing, image generation, machine learning, or decision-making algorithms.
- Generative AI: AI platforms that generate original content such as text, images, video, or audio.
- Non-Public Information: Any data that is private, confidential, proprietary, or otherwise protected by law or policy, including personal information.

4. Governance Structure

Oversight and authority for AI use in city operations are assigned as follows:

- Mayor (Chief Executive Officer): Provides executive oversight and is responsible for enforcement and operational decisions related to AI use.
- City Clerk (Chief Information Officer): Maintains administrative oversight of technology systems and coordinates AI usage compliance.
- City Council: Holds final legislative authority on matters of AI policy, exceptions, and disputes.

All AI-related procurement, deployment, or significant operational use must be disclosed to the Clerk and reported to the Mayor. The City Council reserves the right to review, modify, or revoke AI usage decisions.

5. Authorized Use

The following guidelines must be followed when using AI:

- AI tools may only be used for municipal purposes approved by the City Clerk or Mayor.
- Use of AI must not violate any local, state, or federal laws, including open records laws, intellectual property rights, or privacy regulations.
- AI-generated content used in public communications (e.g., websites, social media, printed materials) must be clearly disclosed when applicable (e.g., "This content was generated using an AI tool").
- Decisions that affect citizen rights, services, or enforcement must not be made solely by AI systems without direct human review and accountability.

6. Prohibited Use

The following uses are expressly prohibited:

- Uploading, inputting, or exposing any Non-Public Information into public AI platforms (e.g., ChatGPT, Google Gemini) without prior authorization.
- Using AI to impersonate individuals, produce misleading or deceptive content, or engage in political campaigning in violation of Wisconsin Act 123.
- Using AI-generated code in production systems without human review and validation.
- Any AI use that results in discriminatory, harassing, defamatory, or unethical behavior.

7. Transparency and Disclosure

- Any AI-generated content used in official communications must include appropriate disclaimers.
- The City of Waterloo will comply with Wisconsin law requiring explicit disclosure when AI is used to generate synthetic media (audio/video/images) used for public or political messaging.

Example disclaimer:
"This message/image/video was generated using an artificial intelligence platform."

8. Incident Reporting

All suspected or confirmed violations of this policy—including misuse, unauthorized AI activity, or data exposure—must be reported immediately to the City Clerk. The Mayor may initiate corrective actions as necessary, and the City Council may review and act on violations as appropriate.

9. Policy Review

This policy shall be reviewed annually or upon substantial changes to AI technology, legal frameworks, or city operations. Amendments shall be approved by the City Council.

Approval

Approved by:

Mayor of Waterloo, Wisconsin
City Clerk
City Council of the City of Waterloo

City of Waterloo Finance, Insurance & Personnel Committee - - Annual Calendar

revised: 12/26/2024

- □ **Meeting night: 3rd Thursday of month at 6:00 pm**
- □ **Monthly recurring: review of disbursements, payroll, and treasurer's reports**

JANUARY □ Review of Department Heads as needed. □ Audit Prep
FEBRUARY □ Audit
MARCH □ Fee Schedule Review
APRIL □ § 53-12 Review of debt schedules & debt refunding opportunities. □ Audit Presentation third Thursday
MAY □ Addressing items raised in financial audit and Workman's Comp audit □ Resolution for carryover after audit is complete
JUNE □ Mayor's Budget start date; build Council consensus for budget policy objectives □ Tax Incremental Finance Districts, review. □
JULY □ Meet with Dept. Heads on Budget Expectation & Concerns □
AUGUST □ Budget deliberation.
SEPTEMBER □ § 53-14 Updating capital improvement plan. □ Budget deliberation.
OCTOBER □ Initial review of calendar year insurance renewal policies. □ Final Committee budget recommendation to full City Council.
NOVEMBER □ Final review of calendar year insurance renewal policies.
DECEMBER □ Review and recommend Current Budget Amendment #2 (July – Dec.)