CITY OF WEST ALLIS
RESOLUTION R-2023-0135

RESOLUTION UPDATING LANGUAGE AND CORRECTING TYPOS IN VARIOUS POLICIES

WHEREAS, certain policies regarding information technology are outdated and unnecessary; and

WHEREAS, a typo in a recently enacted premium pay was located;

NOW THEREFORE, be it resolved by the Council of the City Of West Allis, in the State of Wisconsin, as follows:

SECTION 1: **REPEAL** "1303 Security, Protection, And Emergency Evacuation Procedures" of the City Of West Allis Policies & Procedures is hereby *repealed* as follows:

REPEAL

~~1303 Security, Protection, And Emergency Evacuation Procedures~~ *(Repealed)*

1. PURPOSE: To describe the procedures to be followed by the Information Services Division for the emergency evacuation and security of the Information Services facilities.
2. ORGANIZATIONS AFFECTED: This policy applies to all City of West Allis departments, boards, commissions, and the general public.
3. POLICY: It is the policy of the Information Services Division to follow a uniform set of procedures for the emergency evacuation and security of the Information Services facilities.
4. REFERENCES: None
5. PROCEDURES:
    a. RESPONSIBILITY The Manager of the Information Services Division shall be responsible for making the necessary arrangements for the emergency evacuation and security of the Information Services facilities.
    b. GENERAL POLICIES
        i. It is the policy of the Information Services Division to prepare and implement an evacuation plan for the Information Services facilities in case of an emergency. Such a plan shall provide for the orderly evacuation of the Information Services facilities and utilization of damage control measures to minimize the loss of valuable data stored in such equipment. An evacuation plan would include as a component, a system by which employees of the department would be assigned a number of computer disks to carry with them as they evacuate the facility.
        ii. It is the policy of the Information Services Division to prepare, on a weekly basis, backup of the data stored in the Division's equipment. Such backup is segregated from the Information Services facilities, placed for security reasons in the vault. Copies are also prepared of the computer disks containing quarterly payroll information and the City's master disk of property within municipal boundaries, after the tax roll is completed each year. These copies are placed in a local bank safe deposit box.
        iii. To preserve the confidentiality of sensitive data, the Information Services Division utilizes a system of controlled files by which

terminal access to sensitive data is restricted. For example, access to such sensitive information as crime reports, parking tickets and payroll data, is available only to properly authorized personnel; and terminal access is limited solely to the offices of those individuals.

iv. Employees of the Information Services Division shall respect the confidentiality of information that is processed by the Division.
v. The Information Services facilities will be protected by a security system and have halon protection.
vi. The proper information services equipment will be protected by an uninterruptible power supply (UPS).
vii. All PCs will maintain anti-virus programs and surge protection.

~~**Effective Date**: 1/1/82~~
~~**Revision Date**: 1/1/98~~

SECTION 2: **REPEAL** "1314 Electronic Communication Systems Monitoring Policy" of the City Of West Allis Policies & Procedures is hereby *repealed* as follows:

REPEAL

~~1314 Electronic Communication Systems Monitoring Policy~~ *(Repealed)*

1. PURPOSE: To protect the City's interest in maintaining the integrity of its electronic communication systems, the City has adopted and intends to rigorously enforce its policies regarding use of electronic communication devices in the workplace. The intent of the Policies is to maximize appropriate usage of the electronic communication systems and to ensure they are not used in a way that is disruptive, offensive to others, or contrary to the best interest and government of the City. Within these policies the City has made it clear that employees have no right to privacy with respect to electronic communication devices and that they consent to the City's accessing, intercepting, viewing and otherwise monitoring information (e.g. internet files, e-mail, etc.) contained on/in the electronic communication systems. It is the City's intent to maintain use of the electronic communication devices consistent with the policies, by means of monitoring such devices in accordance with the provisions of this monitoring policy.
2. ORGANIZATIONS AFFECTED: This policy applies to all City of West Allis departments, divisions, offices, boards, commissions, committees, and employees.
3. POLICY: It is the policy of the City to follow this set of procedures for the monitoring of electronic communication systems.
4. REFERENCES: City of West Allis Electronic Communication Policy; City of West Allis E-mail Policy; City of West Allis E-mail Record Retention Policy.
5. PROCEDURES:
    a. RIGHT TO MONITOR The City has the right to, and will exercise the right to continuously access, intercept, view and otherwise monitor the contents of all electronic messages or files and other electronic system activity. This right includes locating substantive information that is not more readily available by some other means, and accessing messages and files which have been deleted but not fully erased from the system. The City will continuously access, intercept, view and otherwise monitor all employee communications indirectly or directly as needed, for, but not limited to, the following purposes:
        i. cost analysis;
        ii. resource allocation;

iii. optimum technical management of information resources; and
iv. detecting use which is in violation of City policies or constitutes illegal activity. The contents of electronic communications properly obtained may be disclosed within the City to those with a legitimate need to know or to law enforcement officials, without the permission of an employee.

b. PROCEDURE FOR MONITORING Monitoring, in accordance with this policy, shall be the responsibility of the Information Services Manager (ISM), under the general direction of the Mayor. This language does not change the supervisory authority of the Director of the Department of Administration & Finance over the Information Services Division. The ISM will routinely monitor employee use patterns to determine whether such patterns may indicate use inconsistent with the City's Electronic Communication Policies. If there is any indication of impropriety, the ISM shall notify the employee's Department Head/Appointing Authority (as defined in section 2.76 of the Revised Municipal Code). If the Department Head/Appointing Authority and the ISM determine that the employee's electronic system activity warrants further investigation, the ISM shall directly monitor the contents of the questionable electronic system activity as a part of such an investigation. The employee's Department Head/Appointing Authority shall be notified when the monitoring will take place and the results thereof. Such monitoring shall be limited to the date, time, source and a small portion of the text (that which is necessary to determine if improper use has occurred). In addition, a Department Head/Appointing Authority may request the ISM to directly monitor a particular employee's use pattern in accordance with this policy if he/she believes that the employee is/may be using an electronic communication device inappropriately contrary to City Policy. If monitoring indicates that an employee has used an electronic communication device inappropriately/contrary to City Policy, the employee's Department Head/Appointing Authority shall meet with the employee to discuss the reason for the monitoring, the results, thereof and to impose discipline, if deemed appropriate, in accordance with City Policy. The ISM shall also refer all monitoring information which may indicate illegal activity to the Chief of Police.

~~**Effective Date**: 05/02/00~~

SECTION 3: **REPEAL** "1315 Identity Theft Prevention And Red Flag Alerts" of the City Of West Allis Policies & Procedures is hereby *repealed* as follows:

REPEAL

~~1315 Identity Theft Prevention And Red Flag Alerts~~ *(Repealed)*

1. PURPOSE:
Pursuant to the Fair and Accurate Credit Transaction Act (FACTA) provisions of the federal Fair Credit Reporting Act, the City of West Allis (City) must take appropriate measures to safeguard Personal Identifying Information and Covered Accounts from Identity Theft. The purpose of this policy shall be to identify the City's response when patterns, practices, or specific activities occur that indicate the possible existence of Identity Theft and to take all reasonable steps to prevent, and mitigate the theft of Personal Identifying Information. As general guidance, this policy will apply to any City account, program, or procedure that allows multiple household or personal

payments or collects, transfers, stores, or records a person's personally identifiable information.

2. ORGANIZATIONS AFFECTED:
   This policy applies to all City of West Allis departments, divisions, offices, boards, commissions, officials and employees.
3. REFERENCES:
   Fair and Accurate Credit Transactions Act of 2003 (16 C.F.R. §681.2)
4. DEFINITIONS:
   a. Covered Accounts are accounts the City offers or maintains for personal, family, or household purposes that involve multiple payments or transactions and include deferred payments for services or property. Covered Accounts may include utility accounts, ambulance accounts, lien/loan accounts or any customer account where the extension of credit is offered resulting in a continuing relationship and therefore subject to provisions of the Fair and Accurate Credit Transaction Act of 2003.
   b. Identity Theft is a fraud committed or attempted using the Personal Identifying Information of another person without authority.
   c. Personal Identifying Information is any person's first name and last name in combination with any other information, that can be used to identify a specific person, so long as the information obtained would be sufficient to permit a person to commit Identity Theft against the person whose information was compromised. Other information may include but not be limited to a Social Security Number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number or address.
   d. Red Flag is a pattern, practice or specific activity that indicates the possible existence of Identity Theft.
5. POLICY:
   a. Pursuant to State and federal law, the City shall adopt the following general administrative rules to identify and detect Red Flags that raise concerns that Personal Identifying Information or Covered Account information is potentially being misused or stolen and outline procedures for safeguarding this information. The policy shall include eight primary areas of compliance:
      i. Personal Identifying Information
      ii. Covered Accounts
      iii. Red Flags
      iv. Safeguarding Personal Identifying Information
      v. Third Party Vendors
      vi. Notice of Theft
      vii. Notice of Security Breach
      viii. Policy Implementation
   b. Personal Identifying Information The City collects a substantial amount of Personal Identifying Information through multiple processes requiring staff to assess and address risks associated with the collection of this information. Departments/divisions are responsible for assessing current compliance and documenting appropriate safeguard practices in writing.
   c. Covered Accounts Covered Accounts may include utility accounts or any customer account where the extension of credit is offered resulting in a continuing relationship. Covered Accounts or any other account where there may be a reasonably foreseeable risk to customers from Identity Theft are subject to provisions of the Fair and Accurate Credit Transaction Act which requires the City to take additional precautions to eliminate the threat of Identity Theft. Before a customer can open an account with the City, staff must make a good faith attempt to verify the identity of the person opening the

account. Prospective applicants who wish to receive a specific service must provide Personal Identifying Information as required by staff.

d. Red Flags Red Flag patterns, practices or specific activities that indicate the possible existence of Identity Theft may include alerts, notifications, or other warnings received from local law enforcement or other governmental organizations. Such information may include a fraud alert or the United States Post Office providing a notice of address discrepancy. Categories of Red Flags associated with customer accounts or the ability to initiate a customer account may include:
    i. inquiries inconsistent with the history and usual pattern of activity of a customer including such things as a recent and significant increase in the volume of inquiries;
    ii. an unusual number of recently established credit relationships;
    iii. a material change in the use of services, or other unusual activity associated with the account;
    iv. an account that was closed for cause or identified for abuse of account privileges;
    v. documents provided for identification that appear to have been altered or forged;
    vi. the photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification;
    vii. other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification;
    viii. other information on the identification is not consistent with readily accessible information that is on file, such as a prior customer file; or
    ix. an application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled. Other potential Red Flags such as the presentation of suspicious information that may include Personal Identifying Information that is inconsistent when compared against other information sources such as:
        (1) an address that does not match any address in the financial system data file;
        (2) a Social Security Number that does not match previous history for the same customer;
        (3) Personal Identifying Information provided by the customer that is not consistent with other Personal Identifying Information provided by the customer;
        (4) Personal Identifying Information provided is associated with known fraudulent activity as indicated by internal or third-party sources;
        (5) an address on an application is the same as the address provided on a fraudulent application;
        (6) a phone number on an application is the same as the number provided on a fraudulent application;
        (7) Personal Identifying Information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources;
        (8) an address on an application is fictitious, a mail drop, or a prison;
        (9) a phone number that is invalid, or is associated with a pager or answering service;
        (10) a Social Security Number provided is the same as that submitted by other persons opening an account or other

customer;

(11) an address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers;

(12) a person opening the account fails to provide all required Personal Identifying Information on an application or in response to notification that the application is incomplete;

(13) Personal Identifying Information provided is not consistent with information that is on file with the City; or

(14) the person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report in response to a challenge question. Unusual or suspicious activity may include:

(A) shortly following the notice of a change of address for a customer account, the City receives a request for the addition of authorized users on the account;

(B) mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's Covered Account;

(C) the City is notified that the customer is not receiving their bill;

(D) payments are made in a manner associated with fraud; or

(E) an existing account with a stable history shows irregularities. The policy shall provide appropriate responses to detected Red Flags to prevent and mitigate Identity Theft. The City Administrative Officer, IT Manager, Department Manager, and City Attorneys office will determine an appropriate response commensurate with the degree of risk posed.

e. Safeguarding Personal Identifying Information The City shall implement and maintain reasonable safeguards to protect the security and confidentiality of Personal Identifying Information, including its proper disposal. In the event a report indicates an information discrepancy, the discrepancy will be reported to the supervisor for further review and verification of the information, including verifying identification in person at the City, if necessary. Staff shall also report to their supervisor when it appears that account documents have been altered or forged when compared to other documents in a customer or employee file. It shall be brought to a supervisor's attention immediately if any customer, employee or applicant presents invalid identification, or identification that appears forged for the purpose of obtaining access to account information. Access to account information will be permitted in person at the City, only after verifying the person's identity through photo identification or by providing information known only to that person. Account information can also be obtained over the Internet with secure password protection. Access to customer account information via telephone or Internet shall require the customer to verify his or her identity using information that would only be known to the customer as reflected in the customer's account. Staff will notify their supervisor and make note in a customer's file when there is a lack of correlation between information provided by a customer and

information contained in a file for the purposes of gaining access to account information. Information will not be given without first clearing any discrepancies in the information provided. In addition, staff will no longer request Personal Identifying Information on certain forms if the data is determined no longer needed for operational purposes. Documents that have reached retention periods will be purged and destroyed in a manner that maintains Personal Identifying Information in a secure manner. Documents with Personal Identifying Information will be stored in locking files or behind locked doors. Any documents containing Personal Identifying Information will be destroyed or shredded prior to disposal. Staff will note unusual use of accounts, or suspicious activities related to accounts and promptly notify their supervisor when there are an unusually high number of inquiries on an account, coupled with a lack of correlation in the information provided by the customer or employee. When a supervisor is notified of a discrepancy, the supervisor will immediately contact (by telephone or email) the City Administrative Officer, IT Manager, Department Manager, and City Attorneys office. The supervisor will then submit a Red Flag Discrepancy Report detailing the event, to the City Administrative Officer, IT Manager, Department Manager and City Attorneys office, within 24 hours. The City Administrative Officer, IT Manager, Department Manager, and City Attorneys office will determine an appropriate response commensurate with the degree of risk posed. Printing Social Security Numbers on any mailed materials unless redacted; or on cards used to access products, services, or City buildings (such as ID cards); or publicly posting or displaying Social Security Numbers is prohibited. Exemptions include requirements by the state of Wisconsin; federal laws, including statute, such as W2s, W4s, 1099s, etc; records that are required by law to be made available to the public; records for use for internal verification or administrative processes; and records used for enforcing a judgment or court order. Staff will monitor transactions and verify the validity of change of address requests, in the case of existing accounts. Staff will not provide Social Security Numbers or Tax Identification Numbers either verbally or in writing, even where a customer is asking for his/her own information. If the City discovers that any of its customers or employees have become a victim of Identity Theft through Personal Identifying Information used by the City in opening or maintaining an account or associated with any document, the City Administrative Officer, IT Manager, Department Manager, and City Attorneys office will take appropriate steps to mitigate the impacts of such Identity Theft. The IT Manager, in consultation with the City Administrative Officer, Department Manager and City Attorneys office, is responsible for safeguarding Personal Identifying Information stored in electronic format and to document safeguard practices in writing.

f. Third Party Vendors The City has various business relationships with third party contractors. Under these business relationships, the third party contractor may have access to customer information covered under this policy. The City will ensure that the third party contractor's work for the organization is consistent with this policy by:
    i. amending City contracts to incorporate these requirements; or
    ii. by determining through written acknowledgment that the third party contractor has reasonable alternative safeguards that provide the same or a greater level of protection for Personal Identifying Information as provided by the organization.
g. Notice of Theft Notice from customers or employees, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with customer or employee information can potentially be a Red Flag for Identity Theft. Upon notice of Identity Theft to a

supervisor, the City Administrative Officer, IT Manager, Department Manager, and City Attorneys office will be notified to determine an appropriate response commensurate with the degree of risk posed.

h. Notification of Security Breach In the event Personal Identifying Information has been subject to a security breach, the City Administrative Officer, IT Manager, or City Attorneys office will notify the Police Department.

i. Implementation Department/division heads whose departments/divisions are responsible for Covered Accounts shall be familiar with this policy and the Identity Theft Protection Acts, shall train their staff who deal with Covered Accounts as to this policy's requirements, and shall meet with their staff to assess current compliance and document appropriate safeguard practices in writing. Employees are responsible for complying with this policy and any internal processes as directed by their department/division. Noncompliance may result in formal disciplinary action up to and including termination of employment. Employees should contact their supervisor if they have questions about compliance with this policy. The Finance Division is responsible for auditing departments/divisions on an annual basis for compliance verification. A security checklist will be provided to each department/division that works with Covered Accounts to act as a guideline to ensure compliance and proper procedures are followed. The checklist will include sections on program elements, employees, safeguarding electronic information, vendor compliance, and information storage and disposal. Upon review and compliance with the checklist, each department/division must return a signed copy to the Finance Department. The City Administrative Officer, IT Manager, Finance Manager and City Attorneys office are responsible for oversight of the program and program implementation.

6. REVIEW AND UPDATE: As new ways are discovered to perpetrate Identity Theft, this policy must be updated to reflect changes in risks to customers, employees and to the safety of the City. This policy shall be reviewed annually in October by the City Administrative Officer, IT Manager, and City Attorneys office and updated as necessary.

~~**Effective Date**: 4/21/09~~

SECTION 4: **AMENDMENT** "1424 Overtime, Compensatory Time, And Premium Pay" of the City Of West Allis Policies & Procedures is hereby *amended* as follows:

AMENDMENT

1424 Overtime, Compensatory Time, And Premium Pay

1. PURPOSE
   To describe the policies and procedures of the City of West Allis in regard to overtime, compensatory time, and premium pay for City employees.
2. ORGANIZATIONS AND PERSONS AFFECTED
   This policy applies to all City of West Allis departments, boards, commissions, and City employees except represented protective service employees.
3. POLICY
   It is the policy of the City to follow a uniform set of procedures in regard to overtime, compensatory time, and premium pay for City employees.
4. REFERENCES
   City of West Allis Revised Municipal Code, Section 2.76 Fair Labor Standards Act (FLSA) City

of West Allis Policies and Procedures Manual, Policy 1205 – Payroll & Time Records City of West Allis Policies and Procedures Manual, Policy 1318 – On-Call City of West Allis Policies and Procedures Manual, Policy 1412 – Holidays City of West Allis Policies and Procedures Manual, Policy 1454 – Work Hours and Schedules

5. DEFINITIONS. In this section, the following terms and phrases shall have the corresponding meanings:

Bilingual	Able to proficiently and fluently interpret and translate, while maintaining intent and meaning, between the English language and either 1) American Sign Language or 2) a non-English language spoken by at least 5% of the City's population as determined by the most recent U.S. Census or American Community Survey.
Compensatory Time	Time off in lieu of overtime pay. Per the FLSA, Compensatory Time accrual for non-exempt employees shall not exceed 240 hours in a calendar year for non-protective service positions and 480 hours for protective service positions. Should compensatory time accrual exceed said hours in a calendar year, the additional time shall be compensated by a cash payment
Emergency Service	Work that must be done immediately to save lives and to protect property and public health and safety, or to avert or lessen the threat of a major disaster. The nature of Emergency Service shall be determined by the Department Head
Exempt Position	A position as evaluated, classified and adopted in the City's Pay Plan which is not entitled to overtime pay per the FLSA
Fair Labor Standards Act (FLSA)	The federal statute that establishes minimum wage, overtime pay, recordkeeping, and youth employment standards. It also establishes criteria for exempt and non- exempt positions
FLSA Overtime	Hours worked in excess of 40 hours per work week by a non-exempt employee
Hours Worked	All time during a work week wherein an employee is necessarily required to be on the employer's premises, on duty, or at a prescribed work place and/or is required or permitted to perform services of benefit to the employer; it does not include paid or unpaid leave time, such as, but not limited to: time off bank usage, extended sick leave bank usage, vacation, random holidays, sick leave, health care appointments, funeral leave, FMLA, or other time off
Non-Exempt Position	A position entitled to overtime pay per the FLSA. Under the FLSA, non-exempt employees are entitled to time and one-half their "regular rate" of pay for each hour worked over the applicable FLSA overtime threshold in the applicable FLSA work period
Premium Pay	Additional pay provided to employees for working certain types of hours or performing certain duties such as, but not limited to, overtime, incentive work, fill-in pay, interim assignment pay, and other miscellaneous premium pays identified herein
Special Service Overtime	Work that must be completed in order to meet statutorily required deadlines, services, or some other duty of similar nature. For use only when extraordinary circumstance exist, and the departmental salary budget has sufficient funds available for the overtime pay. Does not include the performance of routine or regular duties

6. RESPONSIBILITIES
    a. Department Heads
        i. Endeavor to minimize the need for overtime and compensatory time.
        ii. (Reserved).
        iii. Granting of all overtime, compensatory time, and premium pay is at the sole discretion of the Department Head and permission must be granted in advance.
        iv. Determine the nature of Emergency Service.
    b. Employees Employees shall receive advanced permission prior to working overtime, earning premium pay, and working or using compensatory time.
7. OVERTIME PROCEDURES
    a. FLSA Exempt Employees: Employees in FLSA Exempt positions, per the City of West Allis pay schedule adopted by the Common Council, are not eligible for overtime per FLSA. However, said employees shall be allowed flexibility with respect to the hours worked over 45 hours per week (e.g., late arrivals, longer lunches, early departures, and other personal accommodations).
        i. FLSA Exempt Employees, other than those employees in the Executive or Managerial Service, Assistant City Attorneys, Assistant Chief in Fire Department, and Deputy Chiefs in the Police and Fire Departments shall not be compensated with pay for hours worked over 401 but less than 45 hours per work week; however flexibility shall be allowed with respect to the excess hours. In addition, such employees are eligible for compensatory time earned at straight time (i.e., not time and one half or double time) for any regular hours worked in excess of 45[1] hours per week, except in the case of those who work a 4-2 schedule, compensation at straight time shall be earned when hours worked exceeds four (4) hours beyond their normal work schedule for that week.
        ii. Compensatory Time Earned Unless otherwise noted, overtime work shall be credited to a compensatory time account. Compensatory time earned may be used for time off when approved by an employee's Department Head.
        iii. Compensatory Time Paid as Overtime
            (1) In December of each year, an employee will receive payment for all hours of compensatory time in excess of 60 hours that are listed in their account as of the last pay period ending in November of that year.
            (2) Any unused compensatory time earned between the last pay period ending in November through December 31 of that year, which causes the compensatory time accrual to exceed 60 hours, shall be paid out as overtime.
            (3) An employee, with the approval of their Department Head, shall have the option to receive payment for all or any part of the hours in their compensatory time account. Such payment shall be made by the second pay period following the request. All hours to be paid under this section will be subtracted from the employee's account as of such pay period.
        iv. Compensatory Time Carryover
            (1) An employee shall be allowed to carry over a maximum of 60 hours of compensatory time into the next calendar year.
            (2) Under extenuating circumstances, an employee may request and the City Administrator may approve the carryover of more than 60 hours.
            (3) All compensatory time hours carried into the next calendar year shall only be granted as time off. When compensatory time is taken, said time shall first be reduced from the hours that were carried over. At separation of employment, carried over compensatory time shall extend the term of employment.
    b. FLSA Non-Exempt Employees
        i. FLSA Overtime Earned An employee in a FLSA Non-Exempt Position per the City of West Allis pay plan adopted by the Common Council shall be paid overtime at the FLSA rate of one and one-half times their regular rate of pay for Hours Worked in excess of 40 per work week.
        ii. Compensatory Time in Lieu of Overtime
            (1) An employee may request to have hours added to their Compensatory Time account in

lieu of FLSA Overtime pay. In December of each year, an employee will receive payment for all hours of Compensatory Time in excess of 60 hours that are listed in their account as of the last pay period ending in November of that year. An employee shall be allowed to carry over a maximum of 60 hours of Compensatory Time into the next calendar year. All Compensatory Time hours carried into the next calendar year shall only be compensated as time off. When Compensatory Time is taken, said time shall first be reduced from the hours that were carried over.

(2) Employees in the Engineering Department or Police Department, at the discretion of the Department Head, shall be allowed to carry over up to 120 hours in their Compensatory Time account for use as time off only; however, the balance in said account shall be reduced to 40 hours by April 30.

(3) An employee with the approval of their Department Head shall have the option to receive payment for all or any part of the hours remaining in their Compensatory Time account (excluding any hours carried over from the previous calendar year). Such payment shall be made by the second pay period following the request. All hours to be paid under this section will be canceled from the employee's account as of such pay period.

(4) Public Works Department (PW) Employees not assigned on a regular basis to office positions shall be paid for any overtime work unless an employee requests the overtime to be added to their Compensatory Time account.

iii. Double Time- 5-2 Schedule Employees (4-2 Schedule Employees excluded) Overtime at the rate of double their regular rate of pay shall be paid or accrued for all hours worked on Sundays and paid holidays, if not part of the employee's regular work schedule. This provision shall only apply to employees who are required to work on Sundays or holidays if 40 hours paid during the same week. An employee who chooses to work on those days shall not be entitled to double time pay.

c. Part-Time Employees

i. Part-Time FLSA Exempt Employees: Any hours worked in excess of their normal budgeted schedule can either be paid or accrued as compensatory time at straight-time, depending on Department staffing needs, budgetary availability, and Department Head approval.

ii. Part-Time FLSA Non-Exempt Employees Who Work 40 Hours or Less in a Work-Week: Any hours worked in excess of their normal budgeted schedule can either be paid or accrued as Compensatory Time at straight-time, depending on Department staffing needs, budgetary availability, and Department Head approval.

iii. Part-Time FLSA Non-Exempt Employees Who Work More Than 40 Hours in a Work Week: Only with advance approval by the Department Head, Finance Director, and City Administrator, may such employee work in excess of 40 hours. With said approval, such employees shall be paid in cash at straight time up to 40 hours and any such hours worked over 40 hours may either be paid in cash or accrued as Compensatory Time at time and one-half (1½), depending on Department staffing needs, budgetary availability, and Department Head approval.

d. Emergency or Special Service Overtime

i. Executive or Managerial Service Employees: In no case shall an Executive or Managerial Service employee receive Emergency or Special Service overtime or compensatory time.

ii. FLSA Exempt Employees: Overtime at the straight time rate of pay shall be paid for all Emergency or Special Service work or Special Service work performed by employees after reaching 40 hours paid in a week. Employees may request compensatory time in lieu of overtime.

iii. FLSA Non-Exempt Employees: Overtime at the rate of time and one half (1½) the regular rate of pay shall be paid for all Emergency performed by employees after reaching 40 hours paid in a week. Employees may request compensatory time in lieu of overtime.

8. PUBLIC WORK INCENTIVE ROUTE PROCEDURES
    a. Employees shall receive compensation equal to 8 hours of pay on any day designated as an "incentive work" day by the Director of Public Works/Engineering or his/her designee, even though they are allowed to "punch out" prior to completing 8 hours of actual work. Said employees may be required to perform other duties and/or participate in training. When required to perform other duties and/or participate in training during normal working hours (i.e., 7:00/7:30 a.m. to 3:00/3:30 p.m.), said time is considered part of the "incentive work" day and therefore no additional pay is provided. Example: an employee attends training from 7:00 a.m. to 8:00 a.m. and then performs their incentive route collection from 8:00 a.m. to 1:30 p.m. (total of 6.5 hours worked); the employee would receive their regular 8 hours of incentive route pay.
    b. Incentive Refuse Task Rate. Employees working as collectors on incentive routes shall receive an additional $2.00 per hour.
    c. Overtime at the rate of time and one-half (1½) the regular rate of employee pay shall be paid or accrued for all hours spent performing snow/ice control/removal (that is, after their incentive route duties have been successfully completed), between the hours of 7:00/7:30 a.m. and 3/3:30 p.m.; in excess of 8 hours per day; or on Saturday.
    d. Overtime at the rate of double the regular rate of employee pay shall be paid or accrued for incentive work on Sundays or paid holidays.
    e. Incentive Refuse Shortened Work Week Premium. On each day of a shortened work week either due to a Holiday, weather related issue or any other assignment issue, where it may require the collection of refuse/recycling services in a shortened work week/timeframe, the assigned personnel performing such services, working as collectors on an incentive refuse/recycling route and working 125% of a day's assigned route (1¼) or more as necessary for each work day. The assigned collectors shall be compensated an additional 2 hours pay at time and one-half.
9. DEPARTMENT OF PUBLIC WORKS FILL-IN PAY (FIP)
    a. Fill-in Pay (FIP) for PW Employees performing job duties of a higher classification will be granted for one (1) full day of work (as defined within Policy 1454, Work Hours and Schedules, typically eight (8) hours). In other words, there will be no FIP for less than one (1) full day/eight (8) hours and no proration for partial days. FIP work shall generally apply to short-term situations, must be authorized in advance by the Department Head, and shall be documented using regular time processing methods. FIP shall be administered as follows:
    b. To provide additional compensation to those who are filling in for supervisor positions where directions and assignments need to be given, and oversight provided, to staff on days that the permanent supervisor is not available, or other similar assignments that distinctly require a higher level of work to be completed in the regular employee's absence. It is not intended to be paid to employees who are taking over a portion of another employee's work such as answering phones or responding to walk in customers, and other similar duties. Employees filling in for positions 1-2 grades above the employee's position - $20 per day. Employees filling in for positions 3 or more grades above the employee's position - $40 per day.
    c. Guidelines.
        i. If the superintendent is absent, the designated lead will be responsible to cover the superintendent duties - there will be no applicable FIP.
        ii. If the lead person is absent, the superintendent will be responsible to cover the lead duties (an exception may be made if the superintendent justifies the need for fill-in lead duties).
        iii. During a work day where both the superintendent and lead person are absent, the FIP will be awarded at the minimum level for that date; i.e., lead position.
10. INTERIM ASSIGNMENT PAY (IAP)
    a. Interim Assignment Pay (IAP) will be used as "temporary appointments" to higher job classifications and shall generally apply to long-term situations of two (2) weeks' time or more. IAP shall be formally processed using a Personnel Action Form (PAF). All job classifications, except Executive Service, shall be eligible for IAP. When a Department Head is aware of an absence of 30 or more consecutive calendar days, the IAP shall be

paid from the first day of the temporary assignment.

b. The IAP is based on the pay range of the position temporarily being filled, and shall provide at least a 3-5% pay increase over the employee's current pay rate.
c. If a non-exempt employee is temporarily assigned to an exempt position, said employee retains their status as a non-exempt employee.

d. If a temporary assignment extends beyond 90 consecutive calendar days, the Department Head may seek approval from the City Administrator and the Director of Human Resources to extend the appointment. Any temporary assignment extending beyond 180 consecutive calendar days must be approved by the Common Council and re-approved for every additional 90 consecutive calendar days thereafter.
e. In the event an employee assumes a portion of the position's responsibilities, as determined by the Department Head, the Department Head shall prorate the applicable increase based on the percentage of the duties performed as related to the amount and level of difficulty of duties assumed. The Department Head shall document the duties to be performed on the PAF.
f. For an employee receiving IAP, such pay shall not be compensated if that employee is either off of work in a non-working capacity, per 5(f), resulting in off work status past 5 work days. The person receiving IAP shall be compensated at his/her original pay rate prior to receiving the IAP.

11. MISCELLANEOUS PREMIUM PAY
    a. Emergency Service Call Back Pay: All Non-Exempt Employees (except Executive Service Employees) called in to perform Emergency Service shall be paid a minimum of two (2) hours at the employee's regular base hourly rate of pay if such emergency time worked is less than 1.4 hours (or less than 1 hour for work on Sundays/paid Holidays per Section 7(b)(iii). Once an employee works equal to or more than 1.4 hours, all time worked will be compensated at time and one-half; or for Sundays/paid Holidays per Section 7(b)(iii), once an employee works equal to or more than 1 hour, all time worked will be compensated at double time. Scheduled overtime and scheduled call backs do not constitute emergency service call back. The decision as to the emergency nature of the service shall be determined by the Department Head.
    b. Dispatcher Training Task Rate Pay: Employees classified as a Dispatcher (excluding the Dispatcher/Trainer position) shall receive $1.00 per hour for every hour worked training other Dispatchers.
    c. Acting Communications Supervisor (Dispatch Center) Pay: Employees classified as a Dispatcher shall receive $1.50 per hour for every hour worked as an Acting Communications Supervisor.
    d. Watch Duty Pay: PW Employees shall receive $100.00 per week when on Watch Duty. An additional $45.00 per day shall be paid for each paid holiday per Policy 1412 – Holidays, which occurs during the on-call week. Refer to the Department's Standard Operating Procedures manual along with supplements from individual Divisions which list the guidelines and responsibilities for those employees assigned watch duty.
    e. Shift Differential Pay: Shift differential shall not be paid for any position whose work schedule is outside of the normal hours of operation as set by the Revised Municipal Code, Department Head, or building policy.
    f. Voting Equipment Technician Premium Pay: Employees shall receive $0.50 per hour for every hour worked as a Voting Equipment Technician.
    g. IT On-Call Premium: Employees of the IT Department assigned weekly on-call duties and responsibilities shall receive $100.00 per week while on-call. An additional $45.00 per day shall be paid for each paid holiday per Policy 1412 – Holidays, which occurs during the on-call week. Refer to Policy 1318 - On-Call for policies and procedures of the on-call process.
    h. Annual Holiday Pay: Non-represented protective service personnel (Police Classifications: Lieutenant, Captain, Deputy Chief, Chief; Fire Classifications: Battalion Chief, Deputy Chief, Assistant Chief, Chief) working a 5-2 schedule (i.e., Monday-Friday), shall receive an amount equal to 6.26% of their annual pay on or about December 1 of every year; in addition, said personnel shall receive time off with pay for any holiday, covered under Policy 1412-Holidays,

that falls on a scheduled work day. Those said non-represented protective service personnel working a 4-2 schedule (Police) or 24 hour duty (Fire), shall receive 11 days of 8 hour days of 8 hours each paid at time and one-half; however do not receive time off with pay for any holiday covered under Policy 1412-Holidays that fall on a scheduled work day. New employees and existing employees will be compensated on a pro-rated basis computed on time worked during that calendar year.

i. West Allis Resident Incentive Premium Pay: An employee who resides within the City of West Allis shall be granted an additional premium payment determined in the Salary Schedule; no post-dating or pre-dating shall take place. An employee is required to notify their Department Head within twenty-four (24) hours of any change in residency. The Department Head shall submit a PAF to the HR Department within 24 hours of notification.
j. Police Department SWAT Team Pay: Police Department non-represented staff who are members of the SWAT team shall receive an additional monthly payment consistent with represented SWAT team members' monthly payment.
k. Paramedic Pay: Fire Department non-represented officers who hold paramedic certification shall be compensated at the same rate as represented employees of the Department who receive paramedic incentive pay.
l. Master Trade Licenses and Certification Pay: Effective June 1, 2017, an Electrical Mechanic or Plumber holding a Master License from the State of Wisconsin will receive an additional 2% of base pay (Step 1 of applicable position) to be paid over 26 pay periods for attaining and maintaining the Master License when approved in writing by the Director of Public Works. Equipment Mechanics holding a Certification from either a National Institute for Automotive Service Excellence (ASE) or the Structural Welding Certificate from the State of Wisconsin will receive an additional 2% of base pay (Step 1 of applicable position) to be paid over 26 pay periods for attaining and maintaining the certification or license. In addition, the City will pay for recertification, training, continuing education credits, and other fees necessary for the maintenance of said licenses and certifications.
m. Emergency Medical Dispatch Certification Pay: Police Department-Full-time Dispatchers, Police Communication Supervisors, and the Communication Manager holding Emergency Medical Dispatch certification shall receive an annual payment of $300 payable in December.
n. Work Reduction Pay: Fire Department Battalion Chiefs receive work reduction days off, with compensation, due to their 24-hour work schedule. Each Battalion Chief will be credited with 216 hours of work reduction/compensatory time, consisting of nine (9) periods of twenty-four (24) hours each. The effect of the Work Reduction Pay is to reduce the average work week to 51.84 hours, and the basic work year to 2,695.68 hours.
o. Compression Pay Differential for Police and Fire Department Sworn Non-Represented Employees: Compression Pay Differential provides for the following minimum pay difference for employees in such positions:
    i. Fire Chief: 29% above the Captain Max (which is 8% above the Assistant Fire Chief)
    ii. Assistant Fire Chief: 21% above the Captain Max (which is 8% above the Deputy Fire Chief)
    iii. Deputy Fire Chief: 8% above the Captain Max (which is 5% above the Fire Battalion Chief)
    iv. Fire Battalion Chief: 8% above the Captain Max
        (1) Battalion Chiefs work a normal schedule of 51.84 hours per week. Therefore, these positions do not earn regular overtime until greater than 51.84 hours are worked per week. Overtime earned by Battalion Chiefs is at straight time
    v. Police Chief: 29% above the Det. Sgt. Max (which is 8% above the Deputy Police Chief)
    vi. Deputy Police Chief: 21% above the Det. Sgt. Max (which is 8% above the Police Captain)
    vii. Police Captain: 13% above the Det. Sgt. Max (which is equivalent to the Police Lt.)
    viii. Police Lt.: 8% above the Det. Sgt. Max
p. Bilingual Premium Pay: Each bilingual employee shall receive $50 per pay period if the employee is:
    i. A non-probationary, non-sworn, FLSA-nonexempt, regular full-time employee;
    ii. Not required to use a second language in their regular job duties;
    iii. Employed in a customer-facing position;
    iv. Utilizing their bilingual skill in necessary situations at least 10% of hours worked;

v. If interpreting American Sign Language, licensed under Wis. Stat. 440.032.
vi. Approved for premium pay by that employee's Department Head, the HR Director, and the City Administrator.
    (1) Approval is based upon the employee's proficiency, how frequently the employee serves as an interpreter or translator when asked by other employees within and outside the employee's department, and the employee's availability to translate or interpret during non-scheduled work hours and emergencies.

    (2) Approval may be suspended or rescinded if the employee is not rated as performing during a performance review, the employee is reassigned to a different job position, the functions of the job position no longer meet the requirements for this premium pay, the employee does not maintain proficiency, or the employee is off work in a non-working capacity resulting in off work status for an entire pay period.

SECTION 5: **AMENDMENT** "1312 E-Mail Policy" of the City Of West Allis Policies & Procedures is hereby *amended* as follows:

AMENDMENT

1312 E-Mail Policy

1. PURPOSE:
   The City of West Allis (the "City") provides certain employees with systems to send and receive electronic mail (e-mail) so they can work more productively. E-mail gives employees a useful way to exchange ideas, share files, and keep in touch with colleagues, whether they are located in the next room, another City building, or thousands of miles away. The City's e-mail system is a valuable business asset. The messages sent and received on the e-mail system, like memos, purchase orders, letters, or other documents created by employees in the course of their workday, are the property of the City and may constitute public records. This policy explains rules governing the appropriate use of e-mail and sets out the City's rights to access messages on the e-mail system.
2. ORGANIZATIONS AFFECTED:
   This policy applies to all City of West Allis departments, divisions, offices, boards, commissions, committees and City employees.
3. POLICY:
   It is the policy of the City to follow this set of procedures for the use of the City's e-mail system.
4. REFERENCES:
   Electronic Communications Privacy Act of 1986 and its exceptions; Wis. Stats. §19.21; Wis. Stats. §947.0125.
5. PROCEDURES:
    a. ACCESS TO EMPLOYEE E-MAIL
        i. Employees should not have any expectation of privacy with respect to messages or files sent, received, or stored on the City's e-mail system. E-mail messages and files, like other types of correspondence and City documents, can be accessed and read by authorized employees or authorized individuals outside the City. The City reserves the right to review, audit, intercept, access and disclose all messages created, received or sent over the e-mail system for any purpose. The contents of e-mail properly obtained for legitimate business purposes, may be disclosed within the City without the permission of the employee.

Authorized access to employee e-mail by other employees or outside individuals includes, but is not limited to, the following:

(1) Access by the systems administration staff during the course of system maintenance or administration;

(2) Access approved by the employee, the employee's supervisor, or an officer of the City when there is an urgent business reason to access the employee's mailbox - for example, if an employee is absent from the office and the supervisor has reason to believe that information relevant to the day's business is located in the employee's mailbox;

(3) Access approved by the employee's supervisor, the City's Personnel Division, or an officer of the City when there is reason to believe the employee is using e-mail in violation of the City's policies;

(4) Access approved by the City's Personnel Division or the City Attorney's Office in response to the City's receipt of a court order or request from law enforcement officials for disclosure of an employee's e-mail messages.

ii. Except as otherwise noted herein, e-mail should not be used to communicate sensitive or confidential information. Employees should anticipate that an e-mail message might be disclosed to or read by individuals other than the intended recipient(s), since messages can be easily forwarded to other individuals. In addition, while the City endeavors to maintain the reliability of its e-mail system, employees should be aware that a variety of human and system errors have the potential to cause inadvertent or accidental disclosures of e-mail messages.

iii. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message.

iv. The City will continuously access, intercept, view and otherwise monitor all employee communications indirectly or directly as needed, for reasonable purposes. The contents of electronic communications properly obtained may be disclosed within the City to those with a legitimate need to know or to law enforcement officials, without the permission of an employee.

b. PASSWORDS

Each user accesses the e-mail system by means of a personal log-in name and password, which will be selected by the employee and kept on file with the Department Head.

i. Passwords are intended to keep unauthorized individuals from accessing messages stored on the system. From a systems perspective and from the perspective of an e-mail recipient, passwords also establish the identity of the person sending an e-mail message. The failure to keep passwords confidential can allow unauthorized individuals to read, modify, or delete e-mail messages; circulate e-mail forgeries; and download or manipulate files on other systems.

ii. The practice of using passwords should not lead employees to expect privacy with respect to messages sent or received. The use of passwords for security does not guarantee confidentiality. (See Section 5(a), "Access to Employee E-mail").

iii. Passwords should never be given out over the phone, included in e-mail messages, posted, or kept within public view.

iv. Employees are prohibited from disclosing their password, or those of

any other employee, to anyone who is not an employee of the City. Employees also should not disclose their password to other employees, except when required by an urgent business matter (see Section 5(a)(i)(2) of this policy).

c. PERSONAL USE
    i. The city allows limited, occasional, or incidental personal use of its e-mail system during lunch or break times, subject to the following conditions and restrictions:
        (1) Personal use must not:
            (A) Involve any prohibited activity (see Section 5(d));
            (B) Interfere with the productivity of the employee or his or her co-workers;
            (C) Consume system resources or storage capacity on an ongoing basis; or
            (D) Involve large file transfers or otherwise deplete system resources available for business purposes.
        (2) Employees should not have any expectations of privacy with respect to personal e-mail sent or received on the City's e-mail system. Employees should delete personal messages as soon as they are read or replied to. Employees should not store copies of the personal messages they have sent. Because e-mail is not private, employees should avoid sending personal messages that are sensitive or confidential.

d. PROHIBITED ACTIVITIES
    i. Employees are strictly prohibited from sending e-mail or otherwise using the e-mail system in connection with any of the following activities:
        (1) Engaging in personal business or entertainment on City time;
        (2) Engaging in illegal, fraudulent, or malicious activities;
        (3) Engaging in the unlawful use of the e-mail system as set forth in Section 947.0125 of the Wisconsin Statutes (Unlawful use of computerized communication systems);
        (4) Sending or storing offensive, disruptive, obscene, or defamatory material. Materials which are considered offensive include, but are not limited to: any materials which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone’s age, race, creed, color, sex, ancestry, religious or political beliefs, marital status, national origin or disability;
        (5) Annoying or harassing other individuals;
        (6) Using another individual's account or identity without explicit authorization;
        (7) Attempting to test, circumvent, or defeat security or auditing systems, without prior authorization;
        (8) Accessing, retrieving or reading any e-mail messages sent to other individuals, without prior authorization; or
        (9) Permitting any unauthorized individual to access the City's e-mail system.

e. CONFIDENTIAL INFORMATION
    i. All employees are expected and required to protect the City's confidential information. Employees shall not transmit or forward confidential information to outside individuals or companies without the permission of their supervisor and the Systems Administrator. See Section 5(g), Encryption.
    ii. The City also requires its employees to use e-mail in a way that

respects the confidential and proprietary information of others. Employees are prohibited from copying or distributing copyrighted material - for example, software, database files, documentation, or articles - using the e-mail system.

f. RECORD RETENTION
    i. The same rules which apply to record retention for other City documents apply to e-mail. As a general rule, e-mail is a public record whenever a paper message with the same content would be a public record.
    ii. The specific procedures to be followed with respect to the retention of e-mail records is contained in the City's E-Mail Record Retention Policy. The E-Mail Record Retention Policy shall be reviewed by all employees in conjunction with this E-Mail Policy and it shall be incorporated herein as if fully set forth.
g. ENCRYPTION Encrypting e-mail messages or attached files sent, stored, or received on the City's e-mail system is prohibited except where explicitly authorized. Employees are prohibited from using or installing any encryption software without prior permission from the City's Systems Administrator. Employees with a business need to encrypt messages should submit a written request to their supervisor and the Systems Administrator. When authorized to use encryption by their supervisor and the Systems Administrator, employees shall use encryption software supplied to them by the Systems Administrator. Employees who use encryption on e-mail stored on a City computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all the passwords and/or encryption keys necessary to access the e-mail.
h. E-MAIL POLICY VIOLATIONS Employees violating the City's e-mail policy are subject to discipline, up to and including termination. Employees using the e-mail system for defamatory, illegal, or fraudulent purposes and employees who break into unauthorized areas of the City's computer system also are subject to civil liability and criminal prosecution.
i. STANDARD DISCLAIMER All outbound e-mails shall contain the standard disclaimer specified by the City Attorney’s Office as listed in the attached “City of West Allis Disclaimer.” This disclaimer will be automatically appended to all outgoing emails by the City’s e-mail server.

Effective Date: 02/06/98 **Revision Date**: 10/21/14

E-MAIL AND ELECTRONIC COMMUNICATIONS POLICIES

EMPLOYEE NOTICE As an employee of the City of West Allis (the "City"), I recognize and understand that the City's electronic communication systems are provided for conducting the City's business. However, City policy does permit some limited, occasional, or incidental personal use of the equipment and services under certain circumstances. I understand that all equipment, software, messages and files are the exclusive property of the City. I agree not to use the electronic communication systems in a way that is disruptive, offensive, or harmful to others or to the City. I agree not to use pass codes, access a file or retrieve any stored communication other than where authorized. I agree not to copy, send or receive confidential information without prior authorization from my immediate supervisor and the Systems Administrator. I am aware that the City reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the City's electronic communications systems at any time. I am aware that the City may exercise these rights with or without employee notice, and that such access may occur during or after working hours. I am aware that use of a log-in name and password do not guarantee confidentiality, guarantee privacy or restrict the City's right to access electronic communications. I am aware that violations of this policy may subject me to disciplinary action, up to and including discharge from employment, as well as civil and/or criminal liability. I acknowledge that I have read and that I understand the City's policies regarding e-mail and electronic communications. I also acknowledge that I have read and that I understand this notice. _____

_____ Signature of Employee Date

POLICY REMINDER Use of electronic communication systems is controlled by the City's E-mail and Electronic Communication Policies. These systems are provided for **BUSINESS USE**. However, City policy does permit some limited, occasional, or incidental personal use under certain circumstances. The City has the **RIGHT TO MONITOR** all messages and Internet activities. Employees have **NO RIGHT TO PRIVACY** when using these systems. Misuse of the systems may subject employees to discipline up to and including termination and/or loss of access privileges. If you have not reviewed and signed an acknowledgement form for the City's E-mail and Electronic Communication Policies, you may not access these systems. **PRESSING "OK" SIGNIFIES YOU HAVE READ AND ACKNOWLEDGE THE CITY'S E-MAIL AND ELECTRONIC COMMUNICATION POLICIES**

CITY OF WEST ALLIS DISCLAIMER General The City of West Allis is subject to Wisconsin Statutes relating to public records. Email sent or received by City employees are subject to these laws. Unless otherwise exempted from the public records law, senders and receivers of City email should presume that the email are subject to release upon request, and to state record retention requirements.

This email and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to which they are addressed. The recipient should check this email and any attachments for the presence of viruses. The City of West Allis accepts no liability for any damage that may be caused by a virus that may be inadvertently transmitted by this email. If you have received this email in error, please destroy it and notify the sender immediately.

Regarding Contract Language Nothing in this message or its contents should be interpreted to authorize or conclude a binding agreement or contract between the City of West Allis and the recipient of this email and its attachments without the express written confirmation by a City of West Allis employee who is authorized to enter into lawful contracts.

Regarding Legal Advice If this email is from the City of West Allis and is providing legal advice, it may contain information which is privileged, confidential, and protected by attorney client or attorney work product privileges. If you are not the intended addressee, note that any disclosure, copying, distribution, or use of the contents of this message is prohibited.

Regarding Tax Advice Pursuant to Circular 230 promulgated by the Internal Revenue Service, if this email, or any attachment hereto, contains advice concerning any federal tax issue or submission, please be advised that it was not intended or written to be used, and that it cannot be used, for the purpose of avoiding federal tax penalties unless otherwise expressly indicated. 31 CFR Part 10, § 10.35.

Regarding Trade Secrets The information in the email may include trade secrets or privileged or otherwise confidential information. Unauthorized review, forwarding, printing, copying, distributing, or using such information is strictly prohibited and may be unlawful.

PASSED AND ADOPTED BY THE CITY OF WEST ALLIS COUNCIL _____.

	AYE	NAY	ABSENT	ABSTAIN
Ald. Vince Vitale	_____	_____	_____	_____
Ald. Ray Turner	_____	_____	_____	_____
Ald. Tracy Stefanski	_____	_____	_____	_____
Ald. Marty Weigel	_____	_____	_____	_____
Ald. Suzzette Grisham	_____	_____	_____	_____
Ald. Danna Kuehn	_____	_____	_____	_____
Ald. Thomas Lajsic	_____	_____	_____	_____
Ald. Dan Roadt	_____	_____	_____	_____
Ald. Rosalie Reinke	_____	_____	_____	_____
Ald. Kevin Haass	_____	_____	_____	_____

Attest

_____
Rebecca Grill, City Clerk, City Of West Allis

Presiding Officer

_____
Dan Devine, Mayor, City Of West Allis