Employees that are in Safety Sensitive Positions and employees that are required to maintain a Commercial Drivers License (CDL) are subject to the following screening:

- Pre-employment Screening;
- Random Screening;
- Reasonable Suspicion Screening;
- Post-Accident Screening;
- Return-to-Work Screening; and
- Follow-up on positive test results.

An employee that refuses to submit to a screening as stated above will be subject to termination.

Failing a pre-employment drug and alcohol screening or refusal to submit to the drug and alcohol screening will result in the denial of employment.

The City will pay for all drug and alcohol tests given to its employees.

Definitions and Explanations

Safety Sensitive Positions

- An employee that operates or maintains major mechanical, motorized or electrical equipment on a regular, recurring basis;
- An employee that carries a firearm;
- Firefighters.

Pre-Employment Screening

- Drug Test administered to a prospective employee prior to actual hiring or the reinstatement or rehiring of a former City employee.

Random Screening

- All such screens will be unannounced.
- Employees subject to random screening will have an equal chance of being selected every time the selection is conducted. Appropriate safeguards are also present to ensure that the identity of the individual cannot be determined before or at the time of their selection.
- Except for employees who are off-duty, when an employee is randomly selected for screening, he/she will be notified of the screen and instructed to report to the collection site immediately. Employees who are randomly selected when they are off-duty will report to the collection site at the commencement of their next shift.

Reasonable Suspicion Screening

- Reasonable, articulable, and individualized suspicion will exist when an employee's appearance, behavior, speech, or body odors indicate drug or alcohol use, or the withdrawal effects of the same, or a pattern of abnormal or erratic behavior is observed in the employee's work time actions. Such observations must be personally observed and documented by a supervisor or a City official or employee who has received training

covering the physical, behavioral, speech, and performance indicators of possible drug and alcohol use.

- Reasonable cause can be based on a third party observer's report if the report is independently corroborated or if the employee frequently works in an unsupervised environment
- The employee will be escorted by his/her supervisor to the appropriate specimen collection site for the drug and alcohol screen.
- The supervisor will arrange the transportation of the employee to the employee's home at the completion of the screening.
- The employee will be either assigned to a position which does not require safety sensitive functions or the driving of City vehicles, or placed on non-disciplinary leave with pay while awaiting the screening results. If the test result is negative, the employee will be paid for regularly scheduled hours missed while on non-disciplinary leave.

Post-Accident Screening

- Any employee who, while operating a City-owned vehicle, is involved in a vehicular accident while on duty will be required to submit to a drug and alcohol screen as soon as possible, but no later than 2 hours after the accident:
    - Whenever an employee receives a citation for a moving violation involving the accident; or
    - Any person is injured because of the accident and the injuries require immediate medical treatment to the person away from the accident scene; or
    - When an accident results in property damage in the amount of $1,000 or more to the City property or vehicle.
- An employee who is required to take a post-accident drug and alcohol screen may, at the City's discretion, either be assigned to a position which does not require driving City vehicles, or placed on non-disciplinary leave with pay while awaiting the screening results. If the test result is negative, the employee will be paid for regularly scheduled hours missed while on non-disciplinary leave.

Positive Screening Results

A civilian employee who tests positive will be subject to termination. A merit employee of the Police and/or Fire Department who tests positive will be subject to termination pending a Police or Fire Merit Board hearing.

Police/Fire Department Exposure

Any law enforcement officer or firefighter exposed to alcohol and/or illegal drugs in the line of duty will immediately notify his/her supervisor.

Computer Acceptable Use

All computer systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfer protocols ("FTP") are the property of the City. These systems are to be used for business purposes and are not to be used for personal use unless specifically authorized.

Effective security is a team effort involving the participation and support of every City employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment at the City. These rules are in place to protect the employee and the City. Inappropriate use exposes the City to risks including virus attacks, compromise of network systems and services, and legal issues.

The policy applies to employees, contractors, consultants, temporaries, and other workers at the City, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the City.

Employees learning of any use of the City's electronic communication systems that is inconsistent with the requirements of this policy must notify their supervisor of such misuse or violation immediately.

General Use and Ownership

While the City's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the system remains the property of the City. Because of the need to protect the City's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the City.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by department policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

For security and network maintenance purposes, authorized individuals with the City may monitor equipment, systems and network traffic at any time.
The City reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

The City strives to maintain a workplace free of harassment and is sensitive to the diversity of its employees. Therefore, the City prohibits the use of its electronic information systems in ways that are unlawful, disruptive, offensive to others, or harmful to morale. For example, the display or transmission of images, messages, and cartoons that may offend others because of their sex, race, age, national origin, disability, religion, or any other category protected by law is prohibited. Such misuse includes, but is not limited to, ethnic or racial slurs, racial or sexual comments or jokes, or any other communication that shows disrespect for others on the basis of sex, race, national origin, disability, religion, age, or sexual orientation irrespective of whether these statutes are legally protected.

Security and Proprietary Information

Employees must be extremely cautious to prevent computer viruses from infecting the City's computers or computer network or causing computer system problems.

In addition, loading pirated software into the City's computers may create legal liability for the City. Therefore, ***under no circumstances*** may you load unauthorized computer software onto any computer owned or leased by the City. If you wish to load software onto one of the City's computers you must first receive permission from your Department Head. Further, you should never open any electronic mail or attachment from unfamiliar sources. All questions concerning computer software, the City's computer network, or computer viruses should be directed to the Mayor.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed as needed, and user level passwords should be changed at the discretion of the user.

All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the computer or host will be unattended.

Employees should remember that when they are using the City's electronic information systems, they are creating documents that belong to the City. These documents are not private and may be read by other employees and, under some circumstances, by others outside the workplace.

Employees should also be aware that even though a message may be deleted from the system, a record of it may remain either on the daily backups of all data or in other ways. It is possible to re-create a "deleted" message. Therefore, ultimate privacy of messages is not assured to anyone.

Because information contained on portable computers is especially vulnerable, special care should be exercised.

Postings by employees from the City email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the City, unless posting is in the course of business duties.

All computers or hosts used by the employee that are connected by the City system, whether owned by the employee or the City will be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or a Trojan horse code.

Unacceptable Use

Under no circumstances is an employee of the City authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the City owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.)
5. Revealing account password to others or allowing use of account by others. This includes family and other household members when work is being done at home.
6. Using a City computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any City account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning unless prior authorization is obtained.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending message(s) of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, City employees to parties outside the City.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from with the City's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the City or connected via the City network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging

1. Blogging is defined as writing a blog; a blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
2. Blogging by employees, whether using the City's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the City's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the City's policy, is not detrimental to the City's best interests, and does not interfere with an employee's regular work duties. Blogging from the City systems is also subject to monitoring.
3. City's Confidential Information policy also applies to blogging. As such, employees are prohibited from revealing any City confidential or proprietary information, trade secrets or any other material covered by the City's Confidential Information policy when engaged in blogging.

Exemption for Certain Employees

The above activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Hold Harmless Provision and Indemnification

In providing employees with access to the computer systems, the employee agrees to hold the City harmless and agrees to indemnify the City from any and all liability, loss, or damages.

Authorized Use by Law Enforcement

These provisions do not apply to law enforcement officers engaged in criminal investigations as authorized and sanctioned by the City's Police Department.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

City Attorney Communications

Department Heads and other supervisors who receive attorney-client privileged communications from the City Attorney may not disclose those communications to any unauthorized person without first consulting with the City Attorney or obtaining the approval of the City Council.

Unauthorized disclosures of confidential communications with, by, or from the City Attorney, including emails, legal opinions, or other confidential communications that are subject to the attorney-client privilege, harm the City. The purpose of this policy is to protect confidential communications between the City and its attorneys. The determination of whether a communication between the City Attorney and the City is a confidential attorney-client privileged communication requires an interpretation of law as applied to specific facts. For this reason, employees should consult with the City Council and/or the City Attorney before causing to be disclosed to unauthorized persons any communications from the City Attorney.

"Cause to Be Disclosed" or "Unauthorized Disclosure" means the disclosure of a Confidential Communication to an unauthorized person or failure to exercise due care in maintaining the confidentiality of the Confidential Communication.

"City Attorney" means the person appointed by the City Council as the City Attorney and other attorneys working within the same law firm as the City Attorney, and special legal counsel retained by the City Attorney or by the City Council.

"Confidential Communication" means: Any oral or written communications by or from the City Attorney, including but not limited to communications sent by email and any information provided in an executive session, containing the City Attorney's legal opinions, advice, thoughts, mental impressions or conclusions that are given on behalf of the City. "Confidential Communication" does not include information that is required by law to be reported out of an executive session, is authorized by a majority of the City Council to be disclosed, or otherwise is required to be disclosed under the law.

"Unauthorized person" means:

a. With respect to confidential information communicated during an executive session, any person, other than a Council Member (subject to (c) below), not in attendance at the executive session;

b. Any person to whom the oral or written confidential communication is not directed or addressed; or

c. Any person who has a disqualifying conflict of interest in the subject matter of the information contained in the confidential communication.

"Unauthorized person" does not include other City employees when such employees have a need to know the information contained in the confidential communication in order to discharge the duties of their positions for the benefit of the City.

Social Media

You are expected to adhere to the City's Computer Acceptable Use Policy. Only individuals officially designated by the City have the right and authority to speak on behalf of the City or your department. You must clearly state that your views and opinions on your pages are solely your opinion and do not reflect the opinions or views of the City. You also need to understand that First Amendment rights apply when you are contributing to the debate on matters of public concern, but do not apply to topics which are not considered "public concern.". Unless authorized by the Mayor or department, you should under no circumstance disclose confidential material or matters regarding an ongoing investigation.

The Indiana law banning text messaging while operating a motor vehicle became effective July 1, 2011. The law is restricted to the reading, writing and sending of text messages while a vehicle is in motion. Hands-free (voice-activated) texting is permissible. For this guideline, the term text messaging includes all electronic posts, messages or graphics; whether sent by email, instant messaging, social media, cell phone texting or other similar technology.

The City recognizes the benefits of text messaging for convenient and expedient real-time business communications. These modes of communication have the potential to be abused; resulting in such problems as lost productivity, harassment, security concerns and even possible legal liability. You are strictly prohibited from transmitting messages with obscene, profane, lewd, derogatory or potentially harassing/discriminatory content. You must not send messages you know or have reason to believe, may be false or misleading. Any text messages sent using the City's resources should not be considered private. The City reserves the right to monitor all such messages. You should be aware that these messages are subject to disclosure to outside third parties. These parties include the court system and law enforcement agencies. You should report any known or suspected violations of this policy to management for investigation. Violations may result in disciplinary action, up to and including termination.

Cellular Telephone Use

This Cellular Telephone Use Policy is created to provide efficient and consistent standards and procedures for the acquisition, use, and maintenance of cellular telephone technology by employees to whom a cellular telephone has been issued, and to provide effective organizational communication and cost management associated with acquiring and operating cellular telephones.

Administration

The City, in accordance with established organizational policies, will acquire and recommend the placement of cellular telephones into service in those instances where such technology will ensure and/or substantially support the ability of City employees to carry out the basic duties and responsibilities of their jobs when other methods of expedient communication are not available or appropriate. The City will evaluate the service plan and determine the most appropriate and cost effective plan. The City will administer and oversee the cellular telephones and will identify issues and concerns regarding cellular telephone usage to be addressed by Department Heads and/or elected officials.

Minimum Standards and Criteria for Issuance

An employee must meet at least one of the following criteria in order to be assigned a City issued cellular telephone:

1. Department head may request the placement of cellular telephones in City-owned vehicles whose duties and responsibilities require they maintain in constant, though intermittent, contact with private citizens, customers and colleagues and who spend a significant portion of their workday in or in immediate proximity to a motor vehicle.
2. Employees who by title and responsibility routinely serve or are subject to serve in command or field coordinator roles for actual incidents or events, or rehearsals for such, where individual or public safety and well being may be threatened.
3. Employees with whom immediate and direct telephonic communication is necessary in the performance of their professional responsibilities and organizational duties.
4. Departmental 'pool' telephones allocated for shared usage within a department are the responsibility of the Department Head. Department Heads will ensure telephones are allocated as responsibilities warrant and are maintained for proper operation.
5. Employees for whom assigned duties and responsibilities require mobile communication access, and a cellular telephone provides economic or functional benefits over and above other means of mobile communication, such as:
    a. Employees with whom, in the performance of their job, it is necessary to be in 24 hour per day contact;
    b. Employees with whom there is no other means of communication available other than cellular telephone communication;
    c. Employees for whom for the purposes of confidentiality, use of other communication tools is deemed inappropriate;
    d. Employees for whom in the performance of their professional responsibilities the employee's personal safety or the safety of others is at risk;
    e. Employees who, in the performance of their professional responsibilities, are frequently required to supervise activities outside of the normal work place at facilities and sites normally inaccessible; and
    f. Employees who need to be in ready contact with Police and/or Fire personnel.

Use

All employees assigned a cellular telephone must adhere to and sign-off on this Cellular Telephone Use Policy before being allocated a telephone.

Cellular telephones are acquired with public funds and are so acquired to enable City employees to transact the public's business in the most efficient and cost effective method possible. Telephone numbers are the property of the City and are not transferable, and will be used in the same manner and with the same care and stewardship as all public resources.

The use of cellular telephones is to conduct official business. Employees should limit personal telephone calls, in frequency and duration, to the greatest extent possible. This includes incoming as well as outgoing telephone calls. Personal calls should not interfere with an employee's duties and should not impact an employee's productivity. Text messaging and multi-media messaging, if enabled, are limited to official business only. The department head or elected official will advise the employee if text messaging and multi-media messaging are enabled features available for use.

Regardless of whether a City-owned cellular telephone is being used for public or incidental personal purposes, non public safety employees will not initiate a cellular telephone call while they are driving a motor vehicle. Non public safety employees who receive a cellular telephone call while driving a motor vehicle are required to stop the vehicle in a safe location so that communication is held while the vehicle is stopped. The use of "hands free" technology is acceptable as long as it does not interfere with the safe operation of the vehicle. This section will not apply to employees who are passengers in a motor vehicle. Public Safety employees' use of City-owned cellular telephones while driving a motor vehicle will be governed by departmental policy.

FLSA exempt employees assigned cellular telephones will power-on telephones at all times during their workday, while on-call, and while not accessible by other means of telecommunication.

Monitoring

The service provider will send a monthly statement to the appropriate department. The department head or elected official will review the information contained in the cellular telephone statement. By reviewing the monthly statement of cellular telephone activity, the Department Head or elected official may monitor the use of cellular telephones to ensure they are being used appropriately and in accordance with this policy.

In the event that the allotted minutes are exceeded, it is the responsibility of the Department Head or elected official to determine if calls made by the employee are personal or business, in which the employee is responsible for repayment to the City for personal calls.

The Department Head or elected official will be responsible to address inappropriate use, abuse, or failure to adhere to established policies. Inappropriate use of cellular telephones will be reported to the respective Department Head or elected official with a copy to the Mayor.

Employees found to be in violation of this policy will be subject to disciplinary procedures as may be deemed appropriate by the Department Head or elected official.

The City will make provisions for providing cellular telephone communication capabilities to

employees who, on an intermittent basis, meet the criteria for cellular telephone issuance.

The Mayor and/or Department Head or elected official have the right to revoke or deny use, issuance, or assignment of cellular telephones at any time.

The Mayor and/or Board of Public Works and Safety may reevaluate cellular telephone policies and procedures at any time in the best interest of the City.

The employee recognizes and agrees that a City assigned phone remains the property of the City and as such, communications made and/or data stored on said phone is subject to inspection by the Department Head or City official and the employee has no right of or expectation of privacy concerning said cell phone usage.

Open Door / Issue Resolution

In any organization, there will be honest differences of opinion about working conditions, disciplinary action, rules, and other personnel issues. For the City and its employees to succeed, all must be committed to open communication and continually seek opportunities to perform jobs more efficiently and effectively. An open channel of communication is essential to a good work atmosphere.

If your work-related concern(s) does not involve an issue under the Equal Employment Opportunity/Anti-Harassment Policy or disciplinary action, first discuss your concern with your supervisor, who, in most cases, will be able to address your concern. If you feel the first step does not result in satisfactory resolution, communicate your concerns to the Department Head who will review the concern(s) and, if necessary, meet with involved parties to attempt to bring about a mutual understanding or acceptable resolution.

If the second step does not result in satisfactory resolution, bring your concern(s) to the attention of the Mayor in writing. Include in your written comments the names of the involved parties, dates of prior meetings or attempts to resolve the matter, and reasons given for lack of attention or resolution. The Mayor will investigate the concerns raised and take appropriate action.

Concerns Regarding a Department Head's Conduct

If any employee believes that the Department Head has behaved in any way that is unethical or illegal or inconsistent with any specific policy in this handbook, the employee may report that concern in writing within ten (10) days of the circumstances or events to the Mayor's Office. The Mayor will investigate the concerns raised and take appropriate action.

Travel and Expense Reimbursement

An employee may be reimbursed for mileage at the rate approved by the Common Council to be no more than the Federal rate for the use of privately owned automobiles or at a lesser established rate per mile for the use of privately owned motorcycles for official business.

An employee must file an itemized expense report showing the origin and destination of each trip in sufficient detail to account for the mileage claimed. No reimbursements are payable for travel between home and office. Travel expense reports, which include travel expenses, incurred more than thirty (30) days before the voucher date must be accompanied by a letter of explanation detailing the reason the expense report was provide more than thirty (30) days after the expense was incurred. Mileage is payable to only one of two or more employees traveling on the same trip and in the same vehicle. The names of each such person(s) must be listed on the travel voucher. Charges for parking are reimbursable on any day when an employee is entitled to claim reimbursement for mileage. Employees must submit an itemized receipt for any parking fees in excess of One Dollar ($1.00)

The expenses of employees for attending conferences or meetings that are in excess of 50 miles away from the City and require overnight travel will be reimbursed through a claim voucher signed by the employee and Department Head or elected official. The expense claim voucher must include itemized receipts for all expenses during the travel. The daily rate for meals in which overnight travel is required is $35.00 per day. Itemized receipts must be provided as well as the portion of the receipt that includes the amount of gratuity. Gratuity is be reimbursed up to 15% of the bill (prior to tax). Any amount over 15% will be the responsibility of the employee. Lodging will be reimbursed based on the best local rate available for travel that exceeds 50 miles from the City. The employee is required to provide a tax-exempt certificate to the hotel to receive tax exemption at Indiana hotels. Failure to provide the tax-exempt certificate will result in the employee being responsible for the cost of the tax.

Personal expenses incurred in traveling are not reimbursable, including but not limited to, personal telephone calls, laundry, entertainment, and alcoholic beverages.

Use of City

Any employee of the City who is required to operate a City vehicle in the course of their employment will be subject to the following conditions and restrictions:

- Must be able to meet insurability standards/requirements of the City liability insurance provider;
- Maintain a valid Indiana driver's license;
- Periodic record checks at the bureau of motor vehicles at least annually;
- Use of seat belts by all drivers and seat passengers;
- Employees who are required to operate City vehicles during the course of their employment must immediately report any condition that adversely affects their ability to operate such vehicle(s) and/or equipment; and
- Reassignment or other appropriate personnel action in the event of license revocation, suspension or traffic offense conviction.

In addition, employees must use assigned City vehicles for the purpose(s) authorized. Reimbursement for necessary emergency road service and repairs, parking, and highway-related tolls require appropriate receipts for reimbursement.