# Confidentiality and Acceptable Use Policy

## Purpose

Information security, confidentiality, and copyright protection are matters of concern for employees of the City of Chicago ("City") and for all other persons who have access to City computer files and information assets, whether they are employees, independent consultants or third-party vendors. The City maintains information in the form of computerized files for City departments, boards, and agencies as well as other entities. The City utilizes computer software and methodologies created internally and by third parties who are protected by intellectual property, patent, copyright, and trade secret laws. As such, the City is contractually obligated to prevent any and all unauthorized disclosure or use of these information assets.

## Policy

Information Security Office has established the following recipient obligations to protect its personnel, information systems and resources, the City, and its partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

## Recipient's Obligations

A position of trust has been conferred upon every authorized person who, as part of their job function, encounters confidential information to keep this information secure and private. Both City employees and contractors are obligated to recognize and adhere to these responsibilities while on or off the job. Therefore, an employee of the City or a person authorized to access City data files and information is required:

- To follow the City's privacy and security policies, standards, and guidelines including the Information Security and Technology Policy;
- Not to expose customers' or employees' confidential information (such as social security numbers number, driver's license number, and credit card data or account information);
- To maintain credit card data confidentiality and be in full compliance with the current Payment Card Industry (PCI) Data Security Standards (PCI DSS);
- Not to expose protected health information as protected by HIPAA privacy and security rules;
- Not to engage in, or permit unauthorized use of any information in files or programs maintained by the City;
- Not to seek to benefit personally or permit others to benefit personally through the release of confidential information which has come to him/her by virtue of their function or assignment.
- Not to copy, alter, modify, disassemble, reverse engineer, or decompile any intellectual property. Intellectual property that is created for the City by employees, vendors, consultants, and others is property of the City unless otherwise agreed upon by means of third-party agreements or contracts.
- Not to exhibit or divulge the contents of any City record to any person except in the
- conduct of his/her work assignment or in accordance with the policies of the City;

- Not to disclose the specifics of non-public City related business to unauthorized personnel.
- Not to remove or cause to be removed copies of any official record or report from any file from the office where it is kept except in the performance of his/her duties.
- Not to use or request others to use the City's information technology for personal reasons beyond limited personal use as described in the Information Security Policy.
- Not to conduct City business on devices that allow P2P communication (such as music file sharing) without explicit approval from the Department of Assets, Information and Services (AIS).
- To password protect mobile devices issued by the City or those authorized to connect to the City's information technology resources. Examples include but are not limited to smart phones, laptops, and off-site desktops;
- To treat all passwords as Confidential-grade information.
- Not to aid, abet, or act in conspiracy with another to violate any part of this Confidentiality and Acceptable Use Policy.
- To report any violation of this code by anyone to his/her supervisor immediately.

**Enforcement**

Personnel found to have violated this policy will be reported and investigated. The results of the investigation may result in one or all the following actions: immediate revocation of system access and/or user privileges, job counseling, admonishment, revocation of security clearance, disciplinary action, reassignment, discharge, or loss of employment or contract(s), Related civil or criminal penalties.

**Acknowledgement**

I acknowledge that I have received the City of Chicago's Information Security Policy and its Confidentiality and Acceptable Use Policy regarding responsibilities for security and privacy.

Employee/Consultant Signature Date

X_____ _____

Employee/Consultant Name Department/Division or Company

_____ _____

Employee/Consultant Contact Number _____