User Responsibilities Policy

Policy Statement:

This policy establishes practices and regulations to promote and govern the acceptable use of the City of New York's systems, services, and equipment for all city agencies, employees, contractors, vendors, external partners, and general users, to align with the overarching Citywide Information Security Policies. Each user is responsible for ensuring the secure and compliant utilization of resources and proprietary information.

Data Handling:

- **Safeguarding Information:** Users have a responsibility to safeguard information from any unauthorized access and/or activity, to ensure the confidentiality, integrity, and availability of information assets.
  - Data should be classified and handled accordingly (e.g., PUBLIC, CONFIDENTIAL, SENSITIVE).
- **Incident Reporting:** Promptly report any suspicious activity or security incidents to the appropriate entity or IT department.
  - Comply with applicable notifications in the event of a breach of protected information.
- **Mobile Device/Device Security:** Mobile devices issued by the City and/or devices authorized to connect to the City's resources must be password protected.
  - Computers and other devices must never be left unattended while logged in.
  - Maintain system security though timely software updates on devices.
  - Use secure connections when browsing (HTTPS).
- Access to server rooms and data centers should be restricted to authorized personnel only.
- **Secure Transmission:** Confidential information should not be transmitted over email unless encryption is enabled and authorized. Alternatively, utilize approved encrypted tunnels such as a VPN, PPTP, or SSL for secure data transmission.
- **Document Handling:** Printed documents (e.g., printouts, faxes, and photocopies) must be collected in a timely manner. Uncollected items must be destroyed or secured until the proper owners of the documents are available.

Password Management:

- **Complexity requirements:** Passwords must satisfy complexity requirements:
  - **Length:** Between 8-16 characters.
  - **Character Types:** Passwords must include at least one character from each of the following categories:
    - Uppercase (A-Z).
    - Lowercase (a-z).
    - Number (0-9).
    - Special character (!@#$%&).
- **Password Expiration:** Passwords must be changed every 90 days.

- **Password Storage:** Should never be written on paper or stored on easily accessible locations, such as devices, files, or browsers.
- **Password Sharing:** Under no circumstances should passwords be shared with others, including trusted individuals.
- **Unique Passwords:** Use distinct passwords for different accounts, and multifactor authentication (MFA) for added security.

Key Provisions:

- **Access Control:** Users should only be granted access to data and resources that are essential for their job responsibilities, following the principle of least privilege.
- **Compliance:** Users must read and sign the City's Compliance and Acceptable Use agreement prior to being authorized to access the City's information technology and information assets.
- **Data Ownership:** Any data accessed, created, or processed during employment is property of the City of New York.
- **Monitoring and Auditing:** The City reserves the right to monitor and audit user activities on its systems for security and compliance purposes.
- Upon employment termination, the users access rights must be removed from all systems and all City assets must be returned by the employee.

Enforcement:

Any violation of this policy may subject the user to termination of employment, cancellation of contracts, disciplinary action, civil penalties, and/or criminal prosecution.