THE MUNICIPAL HOUSING AUTHORITY FOR THE CITY OF YONKERS

RESOLUTION # 16 OF 2024

October 31, 2024

The following resolution was adopted by a majority during a meeting of the Board of Commissioners of The Municipal Housing Authority for the City of Yonkers on October 31, 2024, proper notice of which was given to, or waived by, each of the members of the Board of Commissioners, and at which a quorum was present:

WHEREAS, The Municipal Housing Authority for the City of Yonkers (the "Authority" or "MHACY") is a New York State public authority that was created to owns and manages public housing and affordable housing complexes located within the City of Yonkers; and

WHEREAS, The MHACY employs over 100 individuals in a number of skills, positions and locations; and

WHEREAS, Over the years, MHACY has developed, adopted and amended various personnel policies, which have been incorporated into the Personnel Policy Manual, most recently approved by the Board of Commissioners in March, 2022; and

WHEREAS, From time to time it is necessary to review and asses the need to add, update and/or amend said policy to reflect the advances in technology and the workplace environment in general; and

WHEREAS, Nowhere are those advances more prevalent than in the area of computer and cell phone usage.

NOW, THEREFORE, BE IT RESOLVED by the Authority's Board of Commissioners hereby approves the recommended changes to the MHACY Personnel Policy Manual by deleting the current Appendix 7, entitled "Code of Conduct for Computers, Phones and other Electronic Equipment and replacing it with Appendix 7-A, entitled "MHACY Cell Phone Policy," and Appendix 7-B, entitled MHACY Computer Use Policy, drafts of both which are annexed hereto.

I, JAMES J. LANDY, the Chair of the Board of Commissioners of THE MUNICIPAL HOUSING AUTHORITY FOR THE CITY OF YONKERS, do hereby certify that the foregoing resolutions were adopted at a meeting of the Board of Commissioners of the Authority held on the date written above.

_____

JAMES J LANDY, CHAIR

The Municipal Housing Authority of the City of Yonkers
Cell Phone Policy

Purpose

Municipal Housing Authority for the City of Yonkers' (from now on referred to as MHACY) CELL PHONE POLICY sets forth policy about cell phone usage. This policy provides guidelines for appropriately using personal and MHACY-issued cell phones in the workplace. It aims to ensure that cell phone use does not interfere with work responsibilities, compromise security, or infringe upon the rights of others.

Applicability

This policy applies to all MHACY employees receiving a cell phone. MHACY employees include full-time or part-time employees. It includes any independent contractor, interns, and consultants with an MHACY-issued cell phone. All employees receiving an MHACY-issued cell phone must sign this agreement confirming their understanding and acceptance of this policy.

Use of MHACY-Issued Cell Phones

General Use at Work

MHACY-issued cell phones are intended for work-related communication only. Employees are responsible for the security and maintenance of their MHACY-issued cell phones. Personal use of MHACY-issued cell phones is prohibited and must not incur additional costs for MHACY or create unsafe work situations. MHACY prohibits employee use of cell phones while at any work site at which the operation of such device would be a distraction to the user and/or could create an unsafe work environment. Such work sites must be secured, or the device used only by an employee must be out of harm's way in such work environments.

Use While Driving

An employee using an MHACY-supplied device or an MHACY vehicle is prohibited from using a cell phone, hands-on or hands-off, or similar device while driving, whether the business is personal or MHACY-related. This prohibition includes receiving or placing calls, text messaging, surfing the Internet, receiving or responding to emails, checking for phone messages, or any other purpose related to your employment responsibilities performed for or attended in the name of MHACY.

MHACY Issued Cell Phones

MHACY may issue phones to employees whose jobs require them to make calls while away from work or to be accessible for work-related matters. Cell phones issued by MHACY are MHACY property. Employees must comply with MHACY requests to make

their MHACY-issued cell phones available for any reason, including upgrades, replacement, or inspection.

Prohibition of Camera Phones

Employees may not use cameras, video and audio recording devices, or the video or recording features of cell phones or other digital devices that contain such capability at work, as this can cause privacy violations and breaches of confidentiality.

Security of MHACY-Issued Cell Phones

Employees must not use cell phones to capture, store, or share confidential company information, client data, or intellectual property. Employees must follow the company's information security policies when using personal or company-issued cell phones to access company networks, systems, or data.

Loss, Theft, and Damage

Employees must immediately report an MHACY-issued cell phone loss, theft, or damage to their supervisor and the IT department. The company may hold employees financially responsible for the loss, theft, or damage due to negligence.

Compliance and Disciplinary Action

Employees who violate this policy may be subject to disciplinary action, including termination of employment or legal action. Employees with concerns or questions regarding this policy should consult their supervisor or the Human Resources department. This policy will be reviewed periodically and updated as necessary. Employees will be notified of any changes to the policy.

I have read and will abide by the conditions of the MHACY Cell Phone Policy as defined herein:

Employee Name: _____

Employee Signature: _____

Date: _____, 20_____

Municipal Housing Authority for the City of Yonkers (MHACY)
Computer Use Policy

Purpose

This policy is of utmost importance as it outlines the acceptable use of computer systems, networks, and data. Its primary goal is to protect the organization's assets and ensure compliance with legal and ethical standards.

This policy also establishes guidelines for properly using computer systems, networks, and other technology resources provided by the Municipal Housing Authority for the City of Yonkers (MHACY). This policy applies to all employees, volunteers, contractors, and other authorized users of the organization's computing resources.

Employees, volunteers, contractors, and other authorized users have no right to privacy regarding their use of MHACY computers. Due to the critical role MHACY's computer network plays in delivering its services, MHACY monitors computer use on a random basis and for investigatory purposes. This monitoring allows MHACY to take snapshots of computer usage and identify unauthorized uses. Anyone found to violate MHACY's Computer Code of Conduct will be subject to disciplinary action and possible termination.

Policy

1. Acceptable Use

MHACY computer systems, networks, and technology resources are only provided for official business purposes. Users must exercise good judgment, maintain professionalism, and use these resources responsibly and ethically.

- **Prohibited Activities:** Users shall not engage in illegal or unethical acts that could damage the reputation or operations of MHACY. This includes, but is not limited to:
  - Unauthorized access to any computer system or network is a serious offense. Any attempt to breach the security of MHACY's systems will result in immediate disciplinary action, including termination of employment or contract. Distribution or storage of illegal, obscene, or offensive content.
  - Activities that infringe upon the intellectual property rights of others.
  - Using its resources for personal gain or political activities.
  - Accessing, downloading, or distributing inappropriate, offensive, or illegal content.
  - For the safety and protection of MHACY's computer equipment, eating or drinking while operating a MHACY computer or peripherals is not allowed.

2. Access

Access to computer systems and networks is granted based on job responsibilities. Users must:

- Authentication: Users should use their unique login credentials to access MHACY systems and not share their credentials with others.
- Authorization: Access permissions are granted based on job roles and responsibilities. Users must not attempt to access systems or data beyond their authorization.
- Account Security: Users should safeguard their accounts and immediately report any unauthorized access or suspicious activity to the IT department.

3. Data Security and Confidentiality

Users must protect the confidentiality, integrity, and availability of MHACY data and information.

- **Password Management**: Users must create strong passwords, change them regularly, and keep them private.
- **Software Installation**: Only IT-approved software may be installed to prevent malware and unauthorized applications.
- **Data Handling:** Sensitive data must not be transmitted or stored on personal devices without authorization and encryption. Users may not transfer or duplicate any data from their computers to an off-site location without the approval of their supervisor.
- **Data Breaches:** Users must immediately report any data breaches, security incidents, or suspicious activities to the IT department.
- **Confidentiality Agreements:** All users must sign confidentiality agreements and adhere to the principles outlined within them.
- **Data Integrity:** Users must not alter or damage any information on the MHACY computer.

4. Internet and Email Use

Internet access and email communication are provided for official MHACY business purposes.

- **Professional Use:** Email communication should be professional and related to MHACY business. Personal use of email should be minimal and must not interfere with work responsibilities.
- **Prohibited Use:** Users must not send unsolicited bulk emails (spam), engage in phishing or other fraudulent activities, or use MHACY email accounts for personal gain or political activities.
- **Monitoring:** MHACY reserves the right to monitor internet and email use to ensure compliance with this policy. Access to inappropriate websites is prohibited. Internet use should be aligned with the organization’s mission and values.

- **Caution:** Be cautious of phishing attempts. Do not open suspicious emails or attachments. Extreme caution must be taken when opening email messages from unknown sources or navigating to unknown sites.

5. **Software and Hardware Use**

Users must ensure the proper use of software and hardware provided by MHACY.

- **Software Installation:** Users must not install, download, or use unauthorized software on MHACY systems. The IT department must approve all software installations.
- **Hardware Maintenance:** Users must not tamper with or attempt to repair MHACY hardware without authorization. Any hardware issues with your computer should be reported immediately to the IT department for resolution.
- **Licensing:** Users must ensure that all software used is appropriately licensed and compliant with MHACY's software licensing policies.

6. **Network Security**

As users, you play a crucial role in ensuring the security and integrity of MHACY networks and systems. Your vigilance is critical to maintaining the safety of our resources.

- **Security Measures:** Users must not bypass or disable security measures implemented on MHACY networks and systems. This includes firewalls, antivirus software, and intrusion detection systems. Only IT-approved software may be installed to prevent malware and unauthorized applications.
- **Incident Reporting:** Users must immediately report any security vulnerabilities or incidents to the IT department.
- **Remote Access:** Access to MHACY networks must be conducted through approved methods and with proper security measures, such as VPNs and multi-factor authentication.

7. **Monitoring and Privacy**

MHACY reserves the right to monitor and log all use of its computer systems, networks, and technology resources.

- **Monitoring:** Monitoring will be conducted in compliance with applicable laws and regulations to ensure the security and proper use of MHACY resources.
- **No Expectation of Privacy:** Users should not expect privacy when using MHACY systems. All activities may be monitored, logged, and reviewed by authorized personnel.

8. Compliance and Enforcement

Users must comply with this policy and all related MHACY policies and procedures.

- It is crucial to understand that violations of this policy may result in disciplinary action, including but not limited to written warnings, fines to reimburse MHACY for damages, suspension, or termination of employment or contract with MHACY. The severity of the action will depend on the nature and frequency of the violation. Legal Action: MHACY reserves the right to take legal action in cases of serious breaches or illegal activities.
- Policy Acknowledgment: By using MHACY computer systems, networks, and technology resources, users acknowledge that they have read, understood, and agree to comply with this policy.

9. Review and Amendments

This policy will be reviewed annually and may be amended as necessary to reflect changes in technology, legal requirements, or MHACY operations.

10. Training

All employees, contractors, and volunteers will receive regular training on MHACY's Computer Use Policy. This training will cover the proper use of technology resources, data security best practices, and the procedures for reporting security incidents.

11. Definitions

- **Sensitive Data:** Any information protected against unwarranted disclosure, including but not limited to personally identifiable information (PII), financial information, and confidential business information.
- **Security Incident:** Any event compromising the confidentiality, integrity, or availability of MHACY's data or systems.
- **Unauthorized Access:** Any access to MHACY's computer systems or data not explicitly granted by the IT department.

12. Remote Work Guidelines

Employees authorized to work remotely must adhere to the same standards of conduct and security as when working on-site. This includes using MHACY-approved VPNs for network access, ensuring that devices are secure and up-to-date, and safeguarding any sensitive data accessed remotely.

13. Data Encryption Standards

- **Encrypt Sensitive Data:** All sensitive data must be encrypted during transmission and when stored. For example, emails containing confidential information must be encrypted before sending.
- **Portable Devices:** Any portable storage devices (e.g., USB drives) that contain sensitive data must be encrypted and stored securely. Do not store sensitive data on personal or off-site devices without proper encryption.
- **Coordination with IT:** If you need assistance with encryption or have questions about data security, contact the MHACY IT department.

I have read and understood the Computer Use Policy. I also understand that my failure to comply with this policy will result in disciplinary action, which may include the termination of my employment or the cancelation of my contract with MHACY.

Employee/Contractor Name: _____
Employee/Contractor Signature: _____
Date: _____