**CITY OF NEW ORLEANS**
**CHIEF ADMINISTRATIVE OFFICE**

**POLICY MEMORANDUM No. 61(R)** **November 16, 2021**

**TO:** **All Departments, Boards, Agencies and Commissions**

**FROM:** **Gilbert A. Montaño, Chief Administrative Officer**

**SUBJECT: ACCEPTABLE USE POLICY**

## I. PURPOSE

The purpose of this Policy is to provide guidance for the acceptable use of computer equipment and information that is utilized, owned, managed, or leased by the City of New Orleans (the "City") and provided for Employee use. Inappropriate use of equipment exposes the City to risks such as data loss, data corruption, unplanned service outage, unauthorized access to City data, and potential legal issues.

## II. SCOPE

This Policy applies to all Users, including City Employees, independent contractors, and all other City workers, including all personnel affiliated with Third Parties. This Policy applies to all computing systems, electronic media and printed materials that are utilized, owned, managed, or leased by the City or the Office of Information & Technology Innovation ("ITI") ("City Resources" or "Technical Resources"). Any violation of this Policy is subject to disciplinary action, up to and including termination.

## III. POLICY

### 1.1 General Requirements

1.1.1 All Users are responsible for exercising good judgment regarding use of City Resources in accordance with City policies and procedures. City Resources may not be used for any unlawful purpose. If you have a question regarding the proper use of Technical Resources, contact the ITI Service Desk at (504) 658-7800.

1.1.2 All City Resources, including handheld or mobile Devices, computing Devices, operating systems, applications, storage media, network accounts, Internet, Intranet, Extranet, and remote access are the property of the City. These systems are to be used for business purposes in serving the interests of City and of City clients and customers during normal operations.

1.1.3 Any personal device used in serving the interests of the City, must be approved by applicable City leadership and the Written Information Security Plan (see Section V for more information).

1.1.4 Any data created or stored on City Resources remains the property of the City. Any personal use of City Resources, including any documents or emails, are also the property of the City and the City makes no guarantee as to the confidentiality in the personal use of City Resources.

1.1.5 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit City Resources per the City's policies and procedures and to confirm compliance.

**1.2 User Accounts**

1.2.1 The City's Users are responsible for the security of data, accounts, and systems under their control.

1.2.2 Passwords must be kept secure and Users must not share account or password information with anyone. For example, do not write passwords down, do not email or text passwords, and always use complex passwords or passphrases.

**Password Guidelines:**

- **Character Length**: Use a minimum of twelve (12) characters.
- **Character Type:** Use at least one (1) each of a combination of alphanumeric characters – uppercase, lowercase, numbers, and symbols.
- **Dictionary Words**: Avoid using a combination of characters that form easily guessed words.

1.2.3 Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this Policy.

1.2.4 Use of shared accounts (the same account for multiple users) is strictly prohibited. **If you believe that you have been granted access to systems or data outside the scope of your employment responsibilities or job function or that you are using a single shared account amongst multiple users, please contact the ITI Service Desk at (504) 658-7800.**

**1.3 Privileged User accounts**

Users with Privileged User accounts (those with more permissions than a standard user account, such as an administrator account, a root account, or an equivalent super-user account) agree to the following:

1.3.1 Individuals with Privileged User accounts understand it is their responsibility to comply with all security measures necessary and assist in enforcing this Policy and the Written Information Security Plan (see Section V).

1.3.2 Privileged User accounts may only be used for valid business functions that require privileged access. Privileged User account users must still abide by the Least Privilege principal and must not access or alter data for which they have not been authorized and/or have no valid business purpose.

1.3.3 Individuals with Privileged User accounts will log in to the City's environment using standard User credentials. Only when required, a User may log in to systems that require privileged account access with their privileged account credentials.

1.3.4 Privileged User accounts may not be used to modify the Individual's standard user account.

1.3.5 Individuals with Privileged User accounts must comply with requirements of the Written Information Security Plan (see section V) prior to modifying any system or user account.

1.3.6 Individuals with Privileged User accounts understand and acknowledge that all Privileged User account activity is closely monitored. Individuals with Privileged User accounts may not use those accounts to modify, alter, or destroy monitoring log data, except as required by their position responsibilities.

**1.4 Security and Access Requirements**

1.4.1 All City computer systems or approved personal Devices used for City business purposes (*e.g.*, PCs, laptops, workstations, tablets, smartphones, etc.) should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less. Mobile Devices will be managed through a mobile device management tool as detailed in CAO Policy Memorandum No. 60(R).

1.4.2 Users shall not create new passwords that are similar to passwords that have been previously used; create passwords that contain any reference to the City in any form (*i.e.*, Saints, Nola, etc.); nor create passwords that contain any personal data, such as any portion of the user ID or name, a spouse's name, or a child's or a pet's name.

1.4.3 Users should secure their workstations by logging off or locking (Control-Alt-Delete or Windows Key + L) the Device when unattended.

1.4.4 Users must exercise due care when transmitting or storing sensitive information. Communications outside of the City network should use mechanisms in accordance with the Written Information Security Plan (see Section V) for protecting confidential or restricted data (*e.g.*, encryption).

1.4.5 Portable computers are especially vulnerable and will be protected by ITI through next generation endpoint protection solutions, which provides anti-malware protection and host-based firewall capabilities, installed and approved by ITI and may not be disabled or modified by the User.

1.4.6 Users must exercise extreme caution when accessing Electronic Media (including, but not limited to, email attachments and external storage Devices) received from outside the City Network.

1.4.7 Users shall take the necessary and appropriate precautions when opening attachments or emails and shall not open or click on attachments or emails when unsure of the legitimacy of the source or sender.

1.4.8 Known incidents or infections from a virus, malware, or other malicious activity should be immediately reported to the ITI Security Team. The Office of Justice Program ("OJP") Program Manager must be notified if the data is subject to a federal DOJ grant project.

1.4.9 Streaming media should only be accessed for business purposes from trusted commercial sites. Streaming media for entertainment purposes on your City Device is prohibited.

1.4.10 Meeting hosts should verify that all meeting attendees are authorized to access the information shared during meetings (including online meetings). Remote meetings security features, such as passcodes or passwords, should be used to restrict access to authorized Individuals. Remote meeting presenters should take care to close, or protect, confidential or restricted data while in "desktop sharing" mode.

1.4.11 Users will take reasonable steps to protect all City property and information from theft, damage, or misuse. This includes maintaining and protecting User workspace, equipment, and information from unauthorized access whether working at City facilities or off-site.

1.4.12 Users must use only authorized instant messenger clients; All other forms of instant messenger software are prohibited.

## 1.5 Virtual Private Network (VPN) Usage

1.5.1 It is the responsibility of Users with VPN privileges to protect their VPN login and account information.

1.5.2 Connections to City Resources via the VPN must originate from City-authorized computing Devices.

1.5.3 Users understand and acknowledge that by using VPN technology the connected computing resource is a de facto extension of the City's Network and as such is subject to the same rules and regulations that apply as if connected locally to the Network.

1.5.4 Connections to non-City VPNs from within a City Network must be specifically authorized and approved in accordance with the Written Information Security Plan (see Section V).

**1.6 External Storage Devices and City Data Storage**

1.6.1 Connections to external storage Devices (*e.g.*, external hard drives, flash drives, etc.) are prohibited, except where authorized by a Department/Agency director for one-time or daily business use.

1.6.2 Final versions of official City documents should be stored within the departmental shared drive either within Microsoft Office 365 or using the on-site drive storage option. Draft versions of work product may be stored on the Employee's Microsoft Office 365 OneDrive. Personal documents and files should not be stored on City devices.

1.6.3 Each department shall employ a standard naming convention system that its Employees shall use when saving records to the Department's shared drive. Such standard naming convention is required to ensure that all current and future Employees can locate records.

**1.7 Physical Security**

1.7.1 Each User must wear their City-issued identification badge on their person in a visible location when they are within a City facility. The identification badge must be properly secured, and a lost badge must be immediately reported to the ITI Service Desk.

1.7.2 Users must facilitate the entry of personnel without identification badges. All visitors must check in at the reception area, wear any identifying badge or sticker as requested by City reception or security personnel, and remain with their designated escort. Visitors are not allowed in the City facilities after hours except with the specific authorization of a Department head.

1.7.3 Users with City-provided equipment must take appropriate measures to protect the equipment from theft, unauthorized use, or other activity that violates the City's Written Information Security Plan (see Section V).

1.7.4 Users with access to confidential or restricted data should maintain a clean desk, pickup printed materials in a timely manner and appropriately secure paper-based data when not in use.

## 1.8 Mandatory Reporting

1.8.1 Users must report suspicious activity, including but not limited to suspected breach or disclosure of private data, suspected lack of physical or technical security controls, and/or any violation of this Policy. If a Security Breach of Personally Identifiable Information ("PII") data occurs or is judged to be imminent, an (OJP) Program Manager should be notified within twenty-four (24) hours.

1.8.2 Users must not use any Device or system that may be involved in a suspected security incident or data breach. Instead users should use alternative communication methods to report the incident to the ITI Security Team and wait for further instructions prior to turning the Device or system off.

1.8.3 Users must immediately report the details of a suspected security activity involving any "confidential" City data—whether the data is on a computer, paper, or the internet—to the ITI Security Team. Users should include the following: contact information, Department involved, brief description of what happened, and general description of the type of data involved and impact of the incident.

## 1.9 Prohibited System and Network Activities

Unless otherwise authorized per ITI security procedures or the Written Information Security Plan (see Section V), Users shall not:

1.9.1 Engage in any activity that is illegal under local, federal, or international law.

1.9.2 Violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City.

1.9.3 Reproduce copyrighted material, without authorization, including digitizing and distributing of photographs from magazines, books or other copyrighted sources, copyrighted music, and installing copyrighted software for which the City or the end user does not have an active license. The use of any recording device, including digital cameras, video cameras, and cell phone cameras, within the premises of any City facilities to copy or record any internal, confidential, or restricted data is prohibited.

1.9.4 Connect network devices, such as wireless access points or personal laptops, to the City's Network environment without proper authorization and approval.

1.9.5 Intentionally introduce malicious programs into the Network or Server (*e.g.*, viruses, malware, worms, Trojan horses, e-mail bombs, etc.).

1.9.6 Reveal account passwords to others or allow use of his/her/their account by others, including family and other household members when the User is working at home.

1.9.7 Use a City computing asset to actively engage in procuring or transmitting material that would violate sexual harassment or hostile workplace laws and/or City Policy.

1.9.8 Make fraudulent offers or testimonials of people, products, items, or services originating from any City issued user account.

1.9.9 Make statements about warranty, expressly or implied, unless it is a part of normal job duties.

1.9.10 Cause Security Breaches or disruptions of network communication. Security Breaches include accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes degrading the performance, depriving authorized access, disabling, or degrading security configurations.

1.9.11 Perform port or security scanning unless prior approval is granted in accordance with the ITI security Policy and Written Information Security Plan (see Section V).

1.9.12 Execute any form of Network monitoring which would intercept data not intended for the User's host unless this activity is a part of the User's normal job/duty.

1.9.13 Circumvent user authentication or security of any host, network, or account.

1.9.14 Interfere with or deny service to any User (*e.g.*, denial of service attack).

1.9.15 Intentionally restrict, disrupt, impair, or inhibit any network node, service, transmission, or accessibility.

1.9.16 Utilize unauthorized peer-to-peer networking or peer-to-peer file sharing.

1.9.17 Utilize unauthorized software, hardware, proxy avoidance websites or services, or any other means to access any internet resource or website that has been intentionally blocked or filtered by the City or ITI Enterprise Security Team.

**Email and Communications Activities**

Unless otherwise authorized per ITI security procedures or the Written Information Security Plan (see Section V), Users shall not:

1.9.18 Send non-business-related unsolicited email messages, text messages, instant messages, or voice mail, including "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

1.9.19 Engage in any form of harassment or discrimination through email or other electronic means.

1.9.20 Use personal email accounts on the City Networks.

1.9.21 Forge, misrepresent, obscure, suppress, or replace another's identity on any electronic communication to mislead the recipient about the sender.

1.9.22 Solicit email from any other email address (*e.g.*, spam, phishing), other than that of the poster's account, with the intent to harass or to collect replies.

1.9.23 Create or forward chain letters, ponzi or other pyramid schemes to a City User, unless specifically requested by such City User.

1.9.24 Post non-business-related messages to large numbers of Usenet newsgroups (*e.g.*, newsgroup spam).

1.9.25 Store City email on personal devices (*e.g.*, home computers, personal laptops, tablets, smartphones, etc.) except as authorized by the ITI Enterprise Security Team.

**1.10 Users of Confidential and Restricted Information**

1.10.1 By signing this Agreement, Users acknowledge that they are aware of and understand the City's policies regarding the privacy and security of individually identifiable health, financial, criminal and other personal information of Individuals and Employees, including the policies and procedures relating to the use, collection, disclosure, storage, and destruction of confidential and restricted data.

1.10.2 Users shall not at any time, during their employment, contract, association, or appointment with the City or after the cessation of such employment, contract, association, or appointment, access or use confidential or restricted data except as may be required in the course and scope of their duties and responsibilities and in accordance with applicable law and corporate and departmental policies governing the proper use and release of confidential or restricted data.

1.10.3 The unauthorized use or disclosure of restricted data shall result in disciplinary action up to and including termination of employment, contract, association, or appointment, the institution of legal action pursuant to applicable state or federal laws; and reports to professional regulatory bodies.

1.10.4 Users further acknowledge that by virtue of their employment, contract, association, or appointment with the City, they may be afforded access to confidential information concerning the operations and practices of a City entity, which shall specifically include, but shall not be limited to, inventions and improvements, ideas, plans, processes, financial information, techniques, technology, trade secrets, manuals, or other information developed, in the possession of, or acquired by or on behalf of the City, which relates to or affects any aspect of the City's operations and affairs ("Confidential Information"). Users agree that they will not use, disclose, or distribute Confidential Information or information derived therefrom except as a part of normal job duties.

1.10.5 Users understand, acknowledge, and agree that nothing contained herein shall be deemed or regarded as an employment contract or any other guarantee of employment and shall not otherwise alter or affect Users' status as at-will employees (or where applicable, Independent contractor) of the City.

## IV. POLICY ENFORCEMENT

Any User found to have violated this Policy may be subject to disciplinary action, up to and including dismissal, or criminal or civil legal actions.

## V. RELATED STANDARDS, POLICIES AND PROCESSES

1.1 **Written Information Security Plan** This document may be provided upon request but is not made widely available as it is a confidential document.

1.2 **Definitions**:

**Agreement** – A legally binding arrangement that is accepted by all parties to a transaction (*e.g.*, Mutual Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA), Data Sharing Agreement (DSA), Memorandum of Understanding (MOU), formal contract, etc.).

**Computing Systems** – Includes all electronic systems, in addition to all computers, servers, network devices, and other computing devices.

**Device** – Any device or system owned, managed, or utilized by the City or the Office of Information Technology & Innovation (ITI) to transmit, store, or process data. Examples include, but are not limited to, laptops, desktops, servers, routers, firewalls, smart phones, PDAs, tablets, USB drives, tablets, monitoring systems, printers, fax machines, copiers, or network storage devices.

**Electronic Media** – Includes electronic and storage media including tapes, disks, CDs, cassettes, DVDs, USB drives, removable storage devices, and portable computing equipment.

**Employee** – Any full-time, part-time, or temporary employee of the City, including interns and student workers employed by the City or its Departments, Boards, Agencies or Commissions.

**Independent Contractor** – Any person or entity that is not an Employee of the City and who provides services to the City pursuant to an independent contractor or consulting agreement.

**Individual** – Any City Employee, Third Party, Independent Contractor, consultant, partner, or supplier.

**Least Privilege** – The principle of least privilege (also known as the principle of least authority) is an important concept in information security, requiring minimal user profile privileges on systems and applications based on users' job necessities.

**Network** – A group of interconnected computers and Network Devices.

**Network Devices** – Include firewalls, routers, switches (managed or unmanaged), wireless routers, wireless access points (managed or unmanaged), wireless controllers, modems, physical taps, and intrusion prevention systems (IPS) or intrusion detection systems (IDS).

**Personally Identifiable Information (PII)** – Information that, when used alone or with other relevant data, can identify an individual.

**Privileged User** – An individual authorized to access the City's enterprise technical Resources and has the capability to alter the properties, behavior, or control of any information system(s), application(s), or network (e.g., a super user, root, or administrator). Additionally, an individual is a Privileged User if granted such elevated access to perform critical business or technical function(s).

**Security Breach** – The successful compromise of security, confidentiality, or integrity of electronic or physical data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to Confidential or Restricted Data maintained, managed, or held in trust by the City, its Departments, Boards, Agencies or Commissions.

**Server** – A computer system that provides services to other client programs and their users, in the same or a different network. A physical or virtual system that provides a service is also a server.

**Third Party** – Any individual or entity that is not either the City or an Employee of the City and is providing a good or service to the City.

**Training** – Efforts focused to review relevant security knowledge and improve or establish skill and competence. The most significant difference between training and awareness is that training

seeks to teach skills that allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues.

**User** – Any Employee, independent contractor, or third party with authorized access to or that interacts with City data or data stored, processed, or transmitted by the City. The user is responsible for using the data in a manner that is consistent with the purpose intended and in compliance with the Information Security Policy while also reporting any intentional or non-intentional violations of the Information Security Policy.

**Visitor** – An individual or entity that is visiting a City facility and is not the City, an Employee of the City, or a Third Party providing a good or service to the City.

## VI. INQUIRIES

Questions concerning this Policy may be addressed to the Office of Information Technology and Innovation, City Hall, Room 3E05, at (504) 658-7800.

GAM/KL/WS/zaf