SUBJECT: **TECHNOLOGY ACCEPTABLE USE POLICY**

1. PURPOSE: The purpose of this policy is to outline the acceptable use of the City's computer system, as defined herein, including computer equipment, cell phones, and IT network at the City of Indio. These rules are in place to protect the employee and the City of Indio. Inappropriate use exposes the City of Indio to risks including virus attacks, compromise of network systems and services, and potential legal liability.

2. SCOPE: The City hereby establishes policies and procedures governing the use by employees, officials and authorized third parties of the computer system, City stipend funded cell phones, and under limited circumstances, personal devices.

3. GENERAL POLICY:

3.1 Network User Accounts: Use of the City's computer resources is only authorized via a City-issued "Network User Account." The City Manager or their designee shall not issue a Network User Account to any user unless the user in question executes an "Acknowledgement of Receipt" in a form substantially similar to that attached to this policy as Exhibit "A." Any network user account that has not been accessed for a period of 60 days will be disabled and any network user account that has not been accessed for a period of 90 days may be deleted, unless the user is out on an approved leave as determined by the Human Resources Department.

3.2 Email Communications: Email communications are governed by the City of Indio's Administrative Policy A-38, Electronic Mail Policy, as well as any relevant Department-specific policies.

3.3 Internet Use: Internet access is provided by the City of Indio in order for staff to conduct official City business. The Internet shall not be used to view, create, or distribute disruptive or offensive images or messaging, pornography, offensive comments regarding race, gender, disabilities, age, sexual orientation, religious beliefs or practices, political beliefs, or national origin, or in any manner that violates local, State, or federal law. Internet traffic is logged by the City of Indio and is subject to periodic review by IT Staff or as requested by Human Resources or City Manager. Staff shall not use the Internet to transfer or distribute Sensitive Personally Identifiable Information except as allowed in Administrative Policy A-39 Handling of Sensitive Personally Identifiable Information.

3.4 Official Business: The City's computer system is dedicated entirely to City use. Its primary purpose and benefit is the enhancement of efficiency, and improvement of service in the public interest. Except as specifically authorized by this policy, users may only use the

computer system for City use. In connection with such use, users shall neither solicit nor persuade others with respect to any outside commercial venture, religious or political cause, or membership/participation in any outside organization not related to official City business.

3.5 City Ownership/Property: The City owns the entire computer system, including any and all electronic data therein, regardless of the physical location or portability of any electronic device using the computer system. User access to the City's computer system is limited and subject to applicable law, this policy and directions of the City Manager.

3.6 City Issued Equipment: On an as-needed basis, the City will issue equipment including, but not limited to, cell phones, laptops, or tablets, to employees to be able to perform work remotely. If City-issued equipment becomes damaged, lost, or stolen it is the user's responsibility to notify the IT Department immediately. Notifications may be forwarded to the Department Head, Human Resources Director, or City Manager. Use of City-issued equipment is subject to this and all other applicable City policies. City-issued equipment must be returned the next business day after a request for return of the equipment has been made or immediately upon separation from the City. Upon return, equipment users must provide any passcodes, passwords, or personal identification number (PIN) to the person who is receiving the city-issued equipment. Users shall not reformat, reset to factory defaults, failback to a previous image, and/or erase content and/or settings; this shall only be done by authorized Information Technology personnel.

3.7 Personal Use: With the sole exception of a City stipend funded cell phone which is regulated by Section 3.8 hereof, use of the City's computer system for anything other than City use is generally prohibited. This general prohibition extends to internet use and email communications. The only permissible use of the City's computer system by an individual user, apart from City use, shall be on a device assigned to the user in question, and shall be limited as follows: A user's personal use of an electronic device assigned to him/her shall be kept to an incidental minimum (e.g., an amount, likely not ever more than five (5) minutes in any given hour, that does not, within the sole reasonable discretion of that user's immediate supervisor and/or department head, materially interfere with the work performance of the user in question). A user's personal files may not be stored or kept on any device that is part of the City's computer system unless their storage or presence on the device in question does not interfere to any degree in the performance of the device in question. Notwithstanding this provision of this policy, each user's immediate supervisor and/or department head, and in the case of an official, the Mayor, shall have the authority to suspend and prohibit all personal use of any electronic device that is part of the City's computer system, including such incidental use as would ordinarily be permissible. In no event should a user's personal files be stored on any network or server drive.

3.8 Approval and Use of City Stipend Funded Cell Phone: The approval for use of a City stipend funded cell phone requires authorization by the City Manager or their designee. The use, outside the course and scope of a user's performance of their City duties, of a

City stipend funded cell phone shall generally not be regulated by Section 3.7 of this policy. However, the City reserves the absolute right and discretion to audit, monitor and restrict the use of each City stipend funded cell phone as follows: No user of a City stipend funded cell phone shall engage in personal use of that phone to a degree or extent that interferes with his/her performance of City duties. When a stipend is supplied in lieu of providing a City issued cell phone, the cell phone shall have sufficient features to allow access to email, calendars, text messaging and data access, and shall otherwise be what is commonly known as a "Smartphone". The current cell phone stipend amount was set by City Council at $100.00 per month on January 25, 2011.

3.9 Use of Personal Devices and Non-City Email Addresses: Personal devices and non-City issued email addresses shall not be used to conduct City business except as noted in Section 3.7. This includes the configuration of City email accounts on a personal device.

3.10 Subject to limited exceptions, all City records, whether in the form of paper, files or electronically stored information, are subject to disclosure under the California Public Records Act (Government Code Section 6250, et seq.) Records created or transmitted on the City's computer system, including personal and non-personal devices, may be subject to public disclosure under the California Public Records Act or in connection with civil or criminal litigation. Users shall not delete any record that must be preserved per this policy.

3.11 Employee Termination/Lay-Offs: Employees who are terminated or laid-off and officials who end their service to the City have no privacy right, no property right, and no right of continued access, as to any file stored on any device within the City's computer system, including personal files stored on any device assigned to the employee in question. The City shall have the absolute right to review, and delete or retain any or all email messages or personal files of a terminated or laid-off City employee remaining on the computer system after the employees separation. When a user leaves City employment, it is the responsibility of the user's department head and the IT Director to ensure that said user's access to the City's computer system is terminated, and that all files and electronic devices are retained by the City.

3.12 Harassment Prohibited: The City prohibits harassment of any kind and the City's computer system shall not be used for such purpose. If any employee or official is harassed or discriminated against through use the City's computer system, that employee or official must immediately report the act of harassment or discrimination to their supervisor or department head. In the case of any official who is harassed or discriminated against, reporting shall be to the Mayor. If an employee or official feels uncomfortable making such a report, or if the employee's supervisor, a department head or an official is the source of the harassment, condones the problem, or ignores the problem, the employee or official in question must immediately report the harassment to the City Manager.

3.13 Offensive Communications: The dissemination of derogatory, defamatory, obscene, disrespectful, sexually explicit, sexually suggestive, unlawful, or otherwise inappropriate internet and/or email communications, is prohibited. The City prohibits the display or transmission of sexually explicit images, messages, or cartoons or any transmission or use of email communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their sex, race, religion, marital status, age, national origin, physical or mental disability, or any other basis, or any communication prohibited by law. The sending or forwarding a copy of these types of offensive communications on the City's computer system is prohibited.

3.14 Unauthorized Use/Tampering: Except as otherwise provided in this policy, electronic snooping or tampering with any electronic device within the City's computer system by any user is prohibited. "Electronic snooping" consists of: (a) unauthorized use of, or attempt to use, another user's Network User Account or password or electronic device, (b) any unauthorized entry, to or attempt to enter, the computer files and communications of another user, (c) any unauthorized entry, or attempt to enter, the encrypted storage of email messages, and/or (d) accessing or intercepting of any other user's electronic communications.

3.15 City Access: The City reserves the absolute right, for any reason, to access, review, disclose, or delete any or all files or electronic information stored or present in the City computer system, or sent from any electronic device within the system to any person via email or other electronic means. This right also applies, to the extent , related to City use, ,to City stipend funded cell phones. This City right shall exist regardless of any prior notice or other notification to any user.

3.16 Electronic Data Back-up: In order to ensure the computer system's function with maximum network efficiency, network reliability and cost-effective operation, the City's network backup tapes and/or any other system-wide data electronic storage devices containing email and electronic data files shall be retained by the City for not less than three (3) weeks or more than two (2) months. These back-up records exist so that the City can restore files in the event of a computer system failure. The City's back-up system only backs up files that are stored on network servers. Files that are created and destroyed on the same day on an individual user's electronic device, (e.g., personal computer, smartphone, etc.), or deleted prior to a back-up "running," are not backed up by this back-up system. Files stored only on an individual user's personal device or City stipend funded cell phone are also not part of the City's network backup system and therefore may not be recovered in the event of system failure.

3.17 Storage of City Data: City data shall not be stored in any personal "cloud" storage accounts including, but not limited to: Google Drive, Dropbox, or OneDrive. If "cloud" storage is required, contact the City IT Department and a City approved account may be issued. Any City data that contains sensitive personally identifiable information must be stored in accordance with the City's administrative policy A-37, Handling of Personally Identifiable Information. USB drives and/or other removable storage should not be used to store City data, without consent of the Department Head's approval.

3.18 Special Rules Regarding Personal Devices and Non-City Email Addresses:

a. In the event that a user: (i) operates a personal device to do City business in lieu of an electronic device that would ordinarily be issued or funded to some degree by the City, including but not limited to a City issued cell phone or a City stipend funded cell phone, or (ii) operates any electronic device, including a personal device, in a manner whereby that user utilizes a non-City email address as a substitute for a City email address that would be part of the City's computer system, that user understands and agrees that such operation may have consequences under this policy.

b. If the use of a personal device, City stipend cell phone, or a non-City issued email address involves City business in any manner, it is the responsibility of the user to maintain the City business records in accordance with this and all other applicable City policies. The user is also responsible to turn over those records to the City Clerk should they separate from the City. Nothing in this Section 3 shall constitute or be deemed to represent a City waiver of any privilege or exemption from production of any record per the California Public Records Act (Government Code Section 6250, et seq.) or in the context of any litigation or legal proceeding.

4. ACCESS TO COMPUTER INFORMATION CONFIDENTIALITY:

4.1 No Confidentiality/Monitoring: Use of the City's computer system including, but not limited to, work on files, internet service, intranet access, and email, is not confidential. The City provides no assurance of privacy with respect to any user's use of any electronic device that is a part of the City's computer system, and expressly reserves the right to access or monitor, with or without notice, any such device at any time.

4.2 No Expectation of Privacy: The City reserves the right to monitor and record individual user files maintained on the computer system, as well as internet and intranet access and usage and email usage, at any time, to the fullest extent permitted by law. No user shall have any expectation of privacy as to their use of any electronic device that is a part of the City's computer system, including intranet access, internet use, and/or email use. The City has software and systems in place that can and will monitor and record all use by each and every user, including, but not limited to, all internal transmissions, internet website visits, intranet access, newsgroups, email messages, computer files, and file transfers into and out of the City's computer system. City representatives may access, audit, and review all activity and analyze any user's usage patterns, and may, for whatever reason, disclose this data to ensure that the City's computer system is devoted to maintaining the highest levels of productivity, efficiency, professionalism, and to ensure that user conduct conforms to the policies and requirements set forth in this policy.

5. ATTORNEY-CLIENT PRIVILEGED COMMUNICATIONS: Some messages sent, received, or stored on the City email system will constitute confidential, privileged communications between the City and its attorneys. Such attorney-client communications shall not be copied, forwarded, or disclosed to anyone without consulting the City Manager and/or the City Attorney in advance.

6. CONFIDENTIAL INFORMATION: Most communication among City employees is not considered confidential. However, certain communications, such as police investigations, personnel records, and emails to and from the City Attorney, may be confidential or contain confidential information. Users shall direct questions about whether communications are a matter of public record or may be confidential to the City Manager, a department head, and/or the City Attorney.

6.1 Users shall exercise caution in sending confidential information via City email as compared to written memoranda, letters or phone calls, because of the ease with which such information may be retransmitted and publicly disseminated. Administrative Policy A-37 governs the sending of sensitive personally identifiable information.

6.2 Users shall not send or forward confidential information to individuals or entities not authorized to receive same, and shall not send or forward same to any person not directly involved with the specific matter giving rise to the confidential information in question. Administrative Policy A-37 governs the sending of sensitive personally identifiable information. Any user who inadvertently sends an email containing confidential information to an unintended recipient shall immediately report the incident to their department head.

6.3 Care should be taken in using email to ensure that messages are not inadvertently sent to the wrong individual. In particular, users should exercise care when using distribution lists to make sure all addressees are appropriate recipients of the electronically stored information transmitted. Users that utilize distribution lists should take measures to ensure that said lists are current.

7. INTELLECTUAL PROPERTY RIGHTS:

7.1 The City retains all copyrights and other intellectual property rights of which it is the legal owner. All copyrights and other intellectual property rights relating to original works created by users in the course and scope of their employment, including their use of City's computer system, are City's exclusive property. To the extent not otherwise transferred to the City in this Section 7.1, each such user hereby assigns to the City, any and all intellectual property rights arising from the user's creation of original works in the course and scope of their employment, including their use of the City's computer system, to the fullest extent permitted by law.

7.2 Transfer of Information: Except as otherwise permitted by law, users shall not post material on internet or intranet services or send material via email that is copyrighted by a party other than the City.

7.3 Except as otherwise permitted by law, City employees shall not download copyrighted materials from these services.

8. COMPUTER SOFTWARE:

8.1 Valid Software Registration or Licensing: Each piece of proprietary software operating on any electronic device within the City computer system must have valid registration and/or licensing. Proprietary software and associated documentation are subject to copyright laws and licensing agreements, and are not to be reproduced by any user without authorization under a licensing agreement. The City shall retain appropriate documentation to substantiate the legitimacy of all software in use on the computer system. Users shall not use unauthorized software on any electronic device within the City computer system.

8.2 Personal Software: User installation and use of privately-owned software, including screen savers and shareware, on any electronic device within the City computer system is prohibited, unless said software is installed with the prior approval of both the department head of the user in question and the IT Director.

9. PASSWORDS:

9.1 A confidential password does not guarantee privacy and shall not prevent the City from retrieving any electronically stored information in compliance with applicable law and/or this policy. Users have no property or privacy right in voice mail or email as a result of password protection. Passwords and codes help the City to secure electronically stored information, but they do not ensure privacy.

9.2 Users should not share their passwords with anyone. Passwords should not be written down and stored on or near the user's computer, monitor or work area. No user shall use, or attempt to use, another user's password or Network User Account. Any user who obtains a password or Network User Account must keep that information confidential. Users shall not share individual network login and password information with others. A user must contact the City's IT Department to reset their password in the event the user forgets their network password. Password unlocks and resets must be made by the user in person or via phone and the new temporary password will only be provided to the user. When the user logs in with the temporary password they must change it immediately.

9.3 Passwords shall not be stored electronically including, but not limited to, in a web browser, text or Word document, spreadsheet, or electronic "Post-It" notes. If a department has need to store passwords the IT Director can recommend an approved password management system.

9.4 Passwords must meet the following complexity requirements. Passwords must be unique going back ten passwords, cannot contain the username, must not be a word in the dictionary, must be at least eight characters in length, and contain a character from

three or the four following categories: English uppercase characters (A through Z), English lowercase characters (a through z), a base 10 digit (0 through 9), or non-alphabetic character (for example, !, #, $, %).

9.5 Users are required to change their password every ninety days. When leaving their workstation, a user should lock their computer screen. An automatic lock will occur after thirty (30) minutes of inactivity and the user will have to enter their password to unlock the device. If a password is entered incorrectly five times the user account will lock automatically for a thirty minutes or until the Information Technology Department unlocks the account.

10. INTERNET ACCESS:

10.1 Use of the internet is a necessary component of users providing effective and efficient public services. The efficient utilization of the internet for communications and research can improve the quality, productivity, and general cost-effectiveness of the City's work force. Internet capability and user access is provided by the City to each user on an "as needed" basis and is a revocable privilege.

10.2 Internet access and use of on-line services are business communication tools made available to certain users in order to enhance efficiency and effectiveness in the performance of job duties and City-related business. Such access and use shall be in accord with generally accepted business practices and current laws. Use of the internet and/or on-line services must be for the purpose of City business activities or relate to information essential to users for the accomplishment of business-related tasks, and/or communication directly related to City business, administration, or practices.

10.3 The City reserves the right to monitor individual user internet access and use of online services for any purpose including, but not limited to, the review, audit, and disclosure of all matters transmitted over the City's computer system or placed in its network storage.

10.4 Acceptable Use of the Internet: Specifically acceptable uses of the internet include: (a) communication and information exchange that is directly related to the City's mission, objectives, and business activities, (b) communication and exchange for professional development, to maintain currency of training or education, or to discuss issues related to a user's work for the City, (c) use for advisory, standards, research, analysis, and professional society activities related to a user's work for the City, (d) announcement of new City laws, procedures, policies, rules, services, programs, information, or activities, and (e) communication with professional associations, public agencies universities, businesses, and/or individuals associated with the facilitation of City business, research, and/or continuing education.

10.5 Unacceptable Use of the Internet: Specifically unacceptable uses of the internet include: (a) more than incidental access of the internet or on-line services for purposes that are unrelated to City business; personal use shall be kept to a minimum, likely never more

than five (5) minutes in any hour, (b) downloading any program, software, or application from the internet or on-line services onto any electronic device in the City's computer system without prior approval from both a department head and the IT manager, and/or without scanning such applications for viruses before they are either run, stored, or accessed, (c) downloading or distributing pirated software or data, (d) deliberately propagating any virus or any other destructive programming, (e) downloading entertainment software or games, (f) uploading to the internet any software licensed to the City or electronically stored information owned or licensed by the City without the prior written authorization from both a department head and the IT Director, (g) releasing and/or disseminating any confidential City information, (h) intentionally introducing the City's computer system to, or experimenting with, malicious computer code, such as computer worms or viruses, (I) transmitting any material or information on the internet or through the use of on-line services in violation of applicable copyright laws or patents, (j) using any Internet access or on-line services that are likely to result in the loss of any user's work, cause congestion on the City's electronic network, or otherwise interfere with or disrupt the efficient function of any component of the City's computer system, and (k) video or audio streaming without prior authorization from both the department head and IT Director.

10.6 Employees shall not log into personal accounts that synchronize data between devices, including but not limited to a personal Google account, Dropbox, One Drive, etc.. These accounts can bring data from your personal device, including but not limited to personal search history, stored passwords, and documents.

11. INTRANET/EXTRANET: The City's intranet (or extranet) shall be used to store all the City's forms and documents that are frequently used by employees for daily business such as agreement templates, policies and procedures, employee information, registration forms, agenda report templates, and personnel forms. All users shall access the City's intranet to obtain copies of these forms and documents.

12. REMOTE ACCESS

12.1 Remote access to the City network may be granted on an as needed basis. To receive remote access the following criteria must be met: Department Head must approve written request, City issued equipment must be used, remote access must use City approved VPN software. If remote access is for a non-exempt employee, the request must include a start and end date for remote access.

13. PENALTIES:

13.1 A user who violates this policy shall be subject to formal disciplinary action up to and including termination from City employment. In addition, any user found to have violated this policy may have their access to computer files, internet, intranet, email, and any electronic device limited or revoked. Unlawful use of any component of the City's computer system, including internet and email services, may result in referral to the appropriate authorities for administrative action and/or civil or criminal prosecution.

13.2 It is the responsibility of each user to ensure that their conduct conforms to the requirements set forth in this policy. Users who are unsure as to whether a contemplated activity or course of conduct constitutes a violation of this policy shall request prior approval and/or clarification from both a department head and the IT Director, or from the City Manager.

14. Related Standards, Policies, and Processes:

14.1 A-37 Handling of Personally Identifiable Information

14.2 A-38 Electronic Mail Policy.

DEFINITIONS

"City" means the City of Indio, the Successor Agency of the City of Indio, Indio Police Department, and the Indio Water Authority, inclusive of all appointed committees and commissions.

"City Manager" means and includes the City Manager of the City and/or their authorized designee(s) for purposes of the administration of this policy.

"City Issued Cell Phone" means a cell phone, including a "Smartphone" issued by City to a user.

"City Stipend Funded Cell Phone" means a "Smartphone," that is funded, in whole or in part, by a City payment to a user under circumstances where the user maintains his/her own account with a cell phone provider but uses the cell phone for City Use.

"City Use" means use, by a City employee, official, or authorized third party, of any electronic device that is a part of the City's computer system while engaged in City business.

"Computer system" means all computers, hardware, software, IT network, and other electronic resources owned, leased, or licensed by the City for City use, email via the City's servers and domain, and the City's website. The City's computer system includes on- site electronic devices and portable electronic devices, including cell phones, issued or funded to any degree by the City for use by an individual user or multiple users, but excludes non-City funded or provided personal devices.

"Electronic" means relating to information technology with electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

"Electronically stored information" means any information that is stored in an electronic system.

"File" means any electronic document or electronically stored information residing or located, in whole or in part, on the City's computer system or in relation to a user's operation of a City stipend funded cell phone. Files include but are not limited to spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, and email or text messages.

"Official" means any elected or appointed official of the City.

"Personal Device" means an electronic device that is the personal property of an individual user, obtained, used and maintained by that user at no cost or expense whatsoever to the City Personal devices do not include City issued cell phones or City stipend funded cell phones.

"Record" means a file in the custody of a City user or on the City's computer system that is kept either (a) because a law requires it to be kept, or (b) because the record in question was made or retained for the purpose of preserving its informational content for future reference and keeping the record in question is necessary and/or convenient to the discharge of a user's duties to the City. Typically if a user who creates a file has, and in the file exercises authority, with respect to the subject matter addressed in the file in question, to make a final decision for the City, or to direct or influence a final decision-maker, that user's file is a record. All records are files, but not all files are records.

"User" means an employee, official or authorized third party engaged in using the City's computer system per this policy.

"Cloud" means an Internet based computer network most often operated by a third party entity.

Previous Policy

Initial: 10-28-10

Updated: 01-05-2014

Updated: 04-04-2022

ACKNOWLEDGEMENT OF RECEIPT

I hereby acknowledge receipt of a copy of the City of Indio's administrative policy called "Technology Acceptable Use Policy" as approved, respectively, on the following date: _____, and also state that I have carefully reviewed and do understand the employee summary of said policies provided to me. I have received answers to any questions that I may have had about said policies' applicability to my work for the City, and I hereby agree to abide by all provisions of these policies.

In executing this acknowledgment (a) I specifically agree that, with the exception of any City stipend funded cell phone, I have no property right or expectation of privacy regarding any aspect of my use of any component of the City's "computer system" as that term is defined and used in the Technology Acceptable Use Policy including, but not limited to, my use of any electronic device (including a City issued cell phone), each computer file that I create, modify or access, internet use, and transmission or receipt of any email message; (b) I further agree that I will not use a City stipend funded cell phone in a way that interferes with my performance of my duty to the City; (c) I understand that, except for minimal personal communications that in no way interfere with my job performance (never more than five (5) minutes in any hour for users who are not also officials), messages transmitted over the City's computer system, including any City issued cell phone, whether on the internet and email, as well as my use of all computer files, must be related to City business; (d) I understand that City security software may record certain information for management use including, but not limited to, the internet address of any site that I visit, and a record of any network activity in which I transmit or receive any kind of file or message; (e) I understand that the City reserves the right to access, audit, and disclose, for whatever reason or purpose, all messages sent through or in storage on the City's computer system, and messages and communications transmitted via any City stipend funded cell phone, to the extent used in the course and scope of my job duties; and (f) I understand that any violation of any of these policies could lead to disciplinary action against me, up to and including termination, and/or administrative action, and/or criminal or civil prosecution.

Signed: _____

Printed Name: _____

Title: _____

Department: _____

Date: _____