ADMINISTRATIVE REGULATION

OFFICE OF THE CITY MANAGER

Number	**606**
Responsible Department	**Information Services**
Established/Effective Date	**November 1, 2023**
Latest Revision Date	**November 1, 2023**
Next Review & Reauthorization Date	**November 1, 2025**

SUBJECT: Network Password & Cyber Security Policy

1. **Purpose:**
The City is committed to building a strong cybersecurity system to maintain, protect, and secure critical IT infrastructure and data systems. To maintain a secure working environment from various cyberattacks and risks throughout the organization and protect our sensitive data and digital assets, this AR establishes standard operating procedures and related guidelines for City employees and Authorized Users.

2. **Authority:** Section 401 of the Huntington Beach City Charter.

3. **Application:** This AR is applicable to all City employees, including elected and appointed officials and any Authorized Users.

4. **Definitions:**
   - **4.1. Cybersecurity:** the practice of protecting computer systems, networks, and data from theft, damage, or unauthorized access.
   - **4.2. Password:** a secret combination of characters used to authenticate or gain access to a resource.
   - **4.3. Phishing:** e-mail phishing is a fraudulent attempt to obtain sensitive information, such as usernames or passwords, by disguising as a trustworthy entity in an email.
   - **4.4. Hacking:** the unauthorized access to or manipulation of computer systems or data.
   - **4.5. Multi-Factor Authentication:** a security process that requires multiple methods of verification to grant access.
   - **4.6. Firewall:** a system that monitors and controls incoming and outgoing network traffic based on predetermined security policies.
   - **4.7. Authorized User**: All elected and appointed officials and City personnel, or any person who has signed the City's AR 605 Policy Agreement Declaration and is approved to utilize the specific system as part of their assigned official duties.

5. **Policy:**
   - **5.1.** To ensure cybersecurity throughout the organization, the City shall establish standard practices for the creation of strong passwords, the protection of those passwords, and

the frequency of changes to passwords. A poorly chosen password may comprise the City's IT network and digital assets.

5.2. The City shall develop and implement the citywide cybersecurity measures based on the best practices in the industry (e.g. the National Institute of Standards and Technology Cybersecurity Framework).

5.3. To prevent identity theft, the City shall not publish a citywide employee directory to the public (this does not apply for point-of-contact employee information for customers). [For more information regarding the City's Identity Theft Prevention Procedures, please refer to AR 312].

6. Responsibilities:

6.1. The Information Services (IS) Department shall be responsible for:

6.1.1. Establishing, updating, and implementing the citywide password policy for City accounts.
6.1.2. Maintaining the usage of Multi-Factor Authentication in instances where it is supported.
6.1.3. Conducting ongoing training and exercises for City employees and Authorized Users to enhance the City's cybersecurity awareness and preparedness
6.1.4. Conducting a cybersecurity risk assessment as appropriate and consulting with the City's Risk Management team to integrate cybersecurity risk management into the citywide Risk Management Program, for risk mitigation and relevant legal and regulatory compliance.
6.1.5. Taking appropriate measures to detect the occurrence of a cybersecurity event and respond promptly.

6.2. All Department Heads shall enforce compliance with this policy among their employees and promote a culture of cybersecurity awareness and preparedness.

6.3. The HR Department shall be responsible for including the information in this AR during the New Employee Onboarding orientation to help ensure all employees are aware of this policy.

6.4. City Employees/Authorized Users, contractors, and vendors shall be responsible for:

6.4.1. The protection of passwords for all their City's accounts, and not allowing others to use their account(s).
6.4.2. Ensuring their computers and other devices are locked when not in use.
6.4.3. Remaining vigilant in identifying potential cybersecurity threats. By promoting a culture of cybersecurity awareness, they play a crucial role in bolstering the organization's defenses against advanced threats and phishing attacks.
6.4.4. Participating and completing cybersecurity training sessions and exercises provided by the IS Department.

6.4.5. Abiding by the City's cybersecurity policies and promptly reporting incidents to the IS Department.

6.5. Violation of the Policy: City Employees who violate this policy may be subject to disciplinary action up to and including termination. City contractors or third-party vendors who knowingly or negligently commits or permits a material violation of this policy may be subject to the termination of the contract in accordance with the City policies, in addition to any legal remedies as applicable.

7. Procedures:

7.1. Passwords Policy

Each Authorized User's primary computer account password shall be changed every 365 days (except Police Department employees). Prompts will occur upon logging onto the network within 14 days of the password's expiration.

To comply with the Department of Justice (DOJ) rules, Police Department employee users shall change their passwords.

7.1.1. **Guidelines for the Creation of Strong Passwords**

Passwords must have a minimum of 8 characters and consist of at least one character in three of four character types.

- Upper case letters
- Lower case letters
- Numbers
- Special characters or symbols (e.g. @,-, !, #, +, &)

The password(s) that City employees and Authorized Users create is the property of the City of Huntington Beach. It shall not be used for any non-City related passwords.

7.1.2. **Password Recommendations:**

- "Unguessable": A password that is not easily guessed will protect your account from all but the most unlikely scenarios. Multiple Words: Use a sequence of random words, which can be easier to remember than a complicated password.
- Unpredictability: Choose words that aren't commonly associated with each other. Avoid using well-known phrases, quotes, or song lyrics.
- Personal Relevance, but Not Obvious: Choose a passphrase that has meaning to you but would be nonsensical or irrelevant to someone else. This can make it easier for you to remember but harder for someone who knows you to guess.
- Avoid Personal Information: Don't use easily accessible information like birthdates, names of family members, or pets.
- Do not use your username as part of your password.

- Maximum Strength: Choose a password of at least 16 characters

7.1.3. **Password Protection Standards**

7.1.3.1. City personnel and Authorized Users shall not share passwords with anyone, including but not limited to administrative assistants, supervisors, or family members.

7.1.3.2. All users shall not reveal passwords in emails, texts, Microsoft Teams chat/instant messages, or any other electronic communication or save passwords on files in any computer system. All passwords are to be treated as confidential City information.

7.1.3.3. City personnel shall not use the "Remember Password" feature included in some applications (e.g. Outlook, Google, etc.)

7.1.3.4. City personnel and all users should not use the same password for City accounts and other non-City accounts (e.g. personnel email account, online banking, etc.). Where possible, City personnel should not use the same password for various City access needs and use different passwords for different accounts.

7.1.4. **Forgotten or Compromised Passwords**

7.1.4.1. After five (5) bad attempts at using a password in the City's network system, users will be locked out of the network and required to call the IS Help Desk at ext. 8888.

7.1.4.2. Compromised accounts and/or passwords are to be reported immediately to the IS Department by calling the IS Help Desk at ext.8888.

7.2. Cybersecurity Guidelines and Restrictions

In addition to password-related policies, the City shall plan and implement various cybersecurity measures throughout the organization. Best practices include but are not limited to:

7.2.1. The IS Department shall regularly apply security patches to operating systems and applications and deploy endpoint protection software.

7.2.2. All City employees and authorized users shall adhere to these guidelines and restrictions:

- Verify the sender's authenticity before opening email attachments and avoid opening attachments from unknown sources. Contact the IS department for assistance if you have any doubt regarding an attachment's safety.
- Immediately report lost or stolen IT devices to the IS Department.
- Contact the IS department immediately if you suspect any of your user accounts are being used by someone other than yourself.
- Do not store confidential data on removable storage devices such as a thumb drive or flash drive.

7.2.3. Phishing

As phishing attacks have become increasingly sophisticated, all City employees and authorized users shall keep these guidelines in mind and follow them

accordingly. Any questions can be directed to the IS Department at ext.8888.

- ***Be aware****:* Expect simulated phishing emails to land in your inbox on an ongoing basis.
- ***Exercise caution***: Approach each email with the same level of scrutiny as you would with any potential phishing attempt. Analyze the email content, scrutinize the sender's address and look for any signs of suspicious activity.
- ***Do not disclose personal or sensitive information***: Under no circumstances should you respond to or provide personal or sensitive information in these simulated phishing emails or any other suspicious emails.
- ***Report suspicious emails***: If you suspect an email to be a phishing attempt, please report it immediately using your *Phish Alert* button in Outlook.
- ***Leverage training resources****:* Take advantage of additional training options that can enhance your knowledge and understanding of cybersecurity best practices. These resources are available by logging into the City's security awareness training portal (currently Knowbe4portal) and selecting the library tab at the top of the screen.

7.3. Training and Resources

7.3.1. During the City's New Employee Onboarding orientation, there shall be a section dedicated to the password and cybersecurity guidelines above, and the reasoning behind the guidelines.

7.3.2. Regular training and exercises shall be conducted by the IS Department as described in section 7.2.3.

Distribution:
All employees may access the Administrative Regulations via the SurfNet or City website: www.huntingtonbeachca.gov/AR.

John Dankha
Chief Information Officer

Approved as to Form
Michael Gates, City Attorney

Eric G. Parra
Interim City Manager

Review Schedule

REVIEW DATE	DEPT. HEAD INITIAL	CITY MANAGER SIGNATURE