

Resolution No. 5 2024

RESOLUTION ADOPTING THE CITY'S COMPUTER PASSWORD POLICY, AND DECLARING AN EMERGENCY.

WHEREAS, the Auditor of State has requested that the City develop and approve a number of documents which it intends to require for the City to emerge from fiscal emergency; and

WHEREAS, pursuant to the Auditor of State's request, the City administration has developed a "Password Policy" in an effort to protect its technology systems and information assets; now, therefore,

BE IT RESOLVED by the Council of the City of Norwood, State of Ohio, that:

SECTION 1. The Council hereby adopts the computer Password Policy, a copy of which is attached as Exhibit A.


SECTION 2. This resolution is hereby declared to be an emergency and a measure necessary for the preservation of the public peace, health, safety, and general welfare and shall be effective immediately upon its adoption. The reason for the emergency is the immediate benefit of having a clear and efficient process by which the City can protect its technology systems and information assets, and the benefit of completing the tasks assigned by the Auditor of State to enable the City of Norwood to emerge from fiscal emergency as soon as practicable.

PASSED 3/12/2024
Date



Joseph S. Geers
President of Council

ATTEST:

Natalie Assaf, the duly appointed Clerk of Council, attests that this resolution was passed at a regular/special meeting of Norwood City Council on the 12th day of March, 2024 in compliance with the rules of Norwood City Council and the laws of the State of Ohio. The foregoing resolution was submitted to the Mayor of the City of Norwood, Ohio for his signature on the 12th day of March, 2024.


Natalie Assaf
Clerk of Council

APPROVED 12 MAR 24
Date


Victor Schneider
Mayor

CERTIFICATION OF PUBLICATION:

Natalie Assaf, the duly appointed Clerk of Council, attests that this resolution was published in the

Cincinnati Enquirer on 3/28/24 and 4/4/24
(Name of Newspaper) (date) (date)



Natalie Assaf
Clerk of Council

1st Reading _____
Date

2nd Reading _____
Date

3rd Reading _____
Date

All 3 Readings 3/12/24
Date

Tabled _____
Date

Vetoed _____
Date



CITY OF NORWOOD, OHIO PASSWORD POLICY

Password Policy:

Passwords are an important part of the City of Norwood's efforts to protect its technology systems and information assets by ensuring that only approved individuals can access these systems and assets. Passwords are used for various purposes at the City. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and network equipment logins.

The City of Norwood Ohio recognizes, however, that passwords have limits as an access control. For some systems, other approved authentication methods that provide higher levels of assurance and accountability than passwords will be used. However, the City of Norwood's key systems continue to utilize passwords as the primary method for authentication and access control. This policy is designed to establish best practices for the composition, lifecycle and general usage of passwords.

Policy Application:

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City facility, has access to the City network, or stores any non-public City information. This policy applies to all City of Norwood's employees that are considered authorized users of the City's systems as defined in the Password Policy.

Systems Covered:

The following systems are covered in this policy:

- Windows Network (Microsoft Windows Active Directory) or systems that utilize Microsoft Windows.
- Excel, Word, PDF, VIP, WEBGAAP, Emails, Paycor

Principles

- Password Confidentiality

To provide authentication effectively, it is essential that a password be known to only the individual user, unless there are delegates to or sharers of accounts. Users will ensure the confidentiality of their passwords at all times.

- Password Construction

To provide system security, a password must meet minimum length and complexity requirements. Because of technology constraints, password construction rules may vary from one system to another, but they will meet (or exceed) these requirements wherever possible. Long and complex passwords may be difficult for users to remember. Therefore this policy provides guidance to end users on how to construct a memorable password that meets (or exceeds) these requirements.

- Password Construction Rules

A password must be made up of:

- ♣ Eight (8) or more characters.

- ♣ At least one uppercase letter.
- ♣ At least one lowercase letter.
- ♣ At least one number (0 through 9).
- ♣ At least one special character (\$, @, # and so on).

A password should not contain:

- ♣ Your first name or your last name.
- ♣ Names of family members, friends, pets, co-workers, fantasy characters, etc.
- ♣ Personal information about yourself or family members. This includes generic information that can be obtained about you very easily, such as birth date, phone number, vehicle license plate number, street name, apartment/house number, etc.
- ♣ Computer terms and names, commands, sites, companies, hardware, or software.
- ♣ Words that are in the dictionary or are a word in any language.
- ♣ Words that are slang, dialect, jargon, etc.
- ♣ Geographical names or places.
- ♣ Letter or number patterns like aaabbb, qwerty,zyxwvuts, 123321, etc.
- ♣ Any of the above spelled backwards.
- ♣ Any of the above preceded or followed by a number (e.g., secret1,1 secret).
- Password Construction Recommendations
 - ♣ A strong password that meets the minimum construction rules will be rather complex. Here are some recommendations on creating a strong password:
 - ♣ Use uppercase letters in random places.
 - ♣ Misspell words.
 - ♣ Construct a password from the initial letters of a favorite quotation, song lyric, movie and so on, capitalizing some letters and substituting a number or special character in an appropriate place.

• Password Change and Reuse

To minimize the window of opportunity for misuse by someone who has discovered a user's password, users will be forced to change their passwords periodically.

A user's new password will be completely different from any recently used password. Users must create a new password that has no more than three (3) characters in common with a previous password.

A user will be free to choose a new password at any time, but a user may not perform multiple changes in quick succession in order to enable continued use of a recently used password.

• Password Change and Reuse Rules

- ♣ A user must change his or her password a minimum of every 90 days.
- ♣ A user may not change his or her password more than once in two (2) days.
- ♣ A user's password must be different from his or her previous four (4) passwords.

• Password Entry

A system will allow five (5) login attempts ("grace logins"). If the password is not correct on the last allowed attempt, then the user's account will be locked out for a 15-minute wait period before it can be accessed again.

Authorized End Users' Responsibilities

If you are an authorized end user of the City of Norwood's software systems, you have the following responsibilities regarding the passwords you use.

Note that these responsibilities apply even if the system does not enforce any specified rules.

- You must keep your password confidential at all times.
- You should not disclose your password to anyone or talk about a password in front of others.
- You should not hint at the format of a password to anyone.
- You should not use a password that you use on any City of Norwood's system on any external system (including Internet banking and social networking services).
- You should not write down your password.
- You should not reveal your password on questionnaires or security forms.
- You should not use the "remember password" feature in any Web browser.
- You should not send a password electronically.
- You should not use any "password keeper" or "password wallet" software or service.
- You must choose a password that meets or exceeds the length and complexity requirements set out in the Password Construction Recommendations.
- You must choose a password that meets or exceeds the other requirements set out in the Password Construction Recommendations.
- You must change your password at least every 90 days.
- You should not use any of your previous four (4) passwords.
- You must choose a new password that has no more than three (3) characters in common with your previous password.
- You should not change your password more than once in two (2) days.

 Reply all |   Delete  Junk |  





Password Policy



Marcus Patterson

Yesterday, 4:00 PM

Tim Garry; Catherine Cornelius; Ken Miracle 

 Reply all | 

Inbox

CITY OF NORWOOD Pa... 
17 KB

 Show all 1 attachments (17 KB) [Download](#)



Action Items



Cat or Tim, can you put this on the next Resolution or Ordinance? Sorry, I don't know which one it should be. This is for the passing of our computer password policy.

Untitled

Marcus Patterson

Thu 3/7/2024 2:05 PM

To: Tim Garry <tgarry@norwoodohio.gov>;

 1 attachments (179 KB)

20240307130343.pdf;

See page 2

If you have any questions or concerns please contact Ken Miracle.



CERTIFIED PUBLIC ACCOUNTANT AND MANAGEMENT CONSULTANTS

Management Letter

City of Norwood
Hamilton County
4645 Montgomery Road
Norwood, Ohio 45212

We have audited the financial statements of the City of Norwood, Hamilton County, Ohio, (the City), in accordance with *Government Auditing Standards* as of and for the year ended December 31, 2022, and have issued our report thereon dated September 25, 2023.

Government Auditing Standards also require that we describe the scope of our testing of compliance with laws and regulations and internal control over financial reporting and report any irregularities, illegal acts, other material noncompliance and significant deficiencies in the internal controls. We have issued a report dated September 25, 2023 on compliance and internal control over financial reporting required by *Government Auditing Standards* as of and for the year ended December 31, 2022.

Office of Management and Budget Uniform Guidance requires that we report all material (and certain immaterial) instances of noncompliance, and significant deficiencies and material weaknesses of internal control, related to major federal financial assistance programs. We have issued a report dated September 25, 2023 on compliance and on the internal controls required by *Office of Management and Budget Uniform Guidance* as of and for the year ended December 31, 2022.

We are submitting for your consideration the following comments on the City's compliance with applicable laws and regulations and on its internal controls. These comments reflect matters that, while in our opinion do not represent material instances of noncompliance or significant internal control deficiencies, we believe represent matters for which improvements in compliance or in internal controls or operational efficiencies might be achieved. Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing the recommendations suggested below. However, these comments reflect our continuing desire to assist your City. If you have any questions or concerns regarding these comments please do not hesitate to contact us.

An asterisk (*) indicates a comment similar to one issued in the prior audit.

Noncompliance

* Ohio Rev. Code, § 733.43

- The City had one bank account not included on the December 31, 2022 reconciliation: The Retiree's Health Care account. The Retiree's Health Care account had a balance of \$85,076 at December 31, 2022.

Reconciliations are an effective tool to help management determine the completeness of recorded transactions and verify all recorded transactions have been deposited with the financial institution.

Members of Council
 City of Norwood
 Management Letter

We recommend the Treasurer properly reconcile their accounts on a monthly basis and provide the City Auditor with information related to bank fees, interest revenue and expenses, or other items not originating in the daily activity of the City recorded by the City Auditor. Variances should be immediately investigated and justified. We also recommend Council or an appointee of Council, review and sign off on the reconciliation indicating approval and promoting timeliness of reconciliations. Failure to accurately prepare and reconcile the accounting records reduces the accountability over City funds and reduces Council's ability to monitor financial activity, increases the risk that errors, theft, or fraud could occur not be detected in a timely manner.

* Ohio Rev. Code, § 5705.41(B), prohibits a subdivision from expending money unless it has been lawfully appropriated.

Fund	Appropriations	Budgetary Expenditures	Variance
Capital Projects Fund I	\$100,000	\$2,119,384	(\$2,019,384)

Failure to properly appropriate funds before they are spent could result in excessive spending leading to deficit fund balances. In addition, prior to recording the appropriations, the Ohio Rev. Code § 5705.40 requires the legislative authority to pass a resolution amending its appropriation measure.

We recommend the City monitor expenditures and appropriations and obtain supplemental appropriations throughout the year as needed.

Internal Control Recommendations



* Security Password Parameters

Users should be granted access to only those computer systems and functions they require to perform their job. To help ensure this, passwords are used to authenticate the identity of the user attempting to gain access to the computer systems. To prevent the integrity of these passwords from being compromised, passwords should be at least six characters in length and be changed periodically. In addition, account lockout and a minimum number of log in attempts should be set.

The City's password minimum lengths are not set to at least six characters and password expiration is not set to at least 90 days. This may cause accounts to be easily accessed or passwords could become known or easily guessed. In addition, not having a minimum number of log in attempts and a lockout duration could increase the risk that someone could log in under someone's user name and have access to data they normally would not have access to.

We recommend each user be assigned a password minimum length of at least six characters in length, the password expiration setting be set to every 90 days, minimum log in attempts be set between three-five and lockout duration be set to zero. Having account lockout set to zero would require an administrator of the network to unlock the user's account.

* Disaster Recovery Plan

To ensure minimal disruption to services, the City/Clerk should maintain a comprehensive disaster recovery plan identifying procedures which permit the Auditor to continue processing information in the event of a disaster. This plan should be tested to ensure it will work as intended by management. In addition, backup tapes should be periodically tested to ensure data availability.

No city department has a disaster recovery plan in place and backup tapes are not tested. The lack of a disaster recovery plan for restoring computer operations could lead to the City's inability to reestablish systems essential to data processing, in an efficient manner.

Members of Council
City of Norwood
Management Letter

We recommend the development of a disaster recovery plan which includes, but not be limited to:

- Recovery Terms, Definitions, and Personnel Responsibilities
- Recovery (Hot/Cold) Site Information and Procedures
- Off-site Materials and Tape/Dataset Listings
- Technical (Hardware/Software) Recovery Procedures and Configurations
- End User Recovery Procedures
- Prioritized Application Recovery List
- Recovery Testing Plan and Maintenance Procedures
- Public Relations Liaison Procedures

The disaster recovery plan should be periodically reviewed and tested to ensure its continued applicability. This review should also ensure personnel are sufficiently trained to carry out procedures necessary to restore functions critical to business operations. In addition, a copy of the plan should be stored at an off-site location.

These comments are intended for the information and use of the Members of Council and management, and are not intended to be and should not be used by anyone other than these specified parties.

J. L. Uhrig and Associates, Inc.

J. L. UHRIG & ASSOCIATES, INC.
Chillicothe, Ohio

September 25, 2023

Committees of Norwood City Council 2024-2025

President Pro-Tem: Susan Hoover

Clerk Pro-Tem: Alexis Royse

Committee of the Whole

Chair: Joseph S. Geers

Members: Emily Franzen
Susan Hoover
Alexis Royse

Sam Bowling
Candace Winterbauer
Jeff Girton
John Breadon

Law, Ordinance, Human Resource, & Compliance

Chair: Alexis Royse

Members: Sam Bowling
Jeff Girton
Susan Hoover

Finance, Budget, Audit, & Claims

Chair: Candace Winterbauer

Members: John Breadon
Emily Franzen
Jeff Girton

Infrastructure: Streets, Parks, Recreation, & Public Places

Chair: Emily Franzen

Members: Sam Bowling
Alexis Royse
Candace Winterbauer

Small Business & Economic Development

Chair: Sam Bowling

Members: Emily Franzen
Jeff Girton
Susan Hoover

Housing, Health, Environment, & Public Safety

Chair: Susan Hoover

Members: John Breadon
Alexis Royse
Candace Winterbauer