ORDINANCE NO. 2025 – 50 AMENDED

AN ORDINANCE ADOPTING A CYBERSECURITY POLICY FOR THE CITY OF WICKLIFFE, OHIO~~; AND DECLARING AN EMERGENCY~~

WHEREAS, the City of Wickliffe recognizes the importance of establishing clear and consistent policies to guide municipal operations; and

WHEREAS, the Cybersecurity Policy has been reviewed and recommended by the Law Director of the City of Wickliffe, Ohio; and

WHEREAS, City Council finds it to be in the best interest of the City to formally adopt and implement said policy to ensure transparency, consistency, and compliance with applicable laws as well as to safeguard public funds form cybersecurity and ransomware incidents;

NOW, THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF WICKLIFFE, COUNTY OF LAKE, AND STATE OF OHIO:

SECTION 1. The City of Wickliffe hereby adopts the document entitled "Cybersecurity Policy for the City of Wickliffe, Ohio", a copy of which is attached hereto and made a part hereof as *Exhibit A*.

SECTION 2. This policy shall apply to all [employees, departments, contractors, etc.] of the City of Wickliffe and shall take effect immediately upon passage unless otherwise stated in the policy document.

SECTION 3. The Mayor, or their designee, is authorized to take any necessary administrative actions to implement and enforce this policy.

SECTION 4. If any section, clause, or provision of this ordinance is declared invalid by a court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of this ordinance.

SECTION 5. That it is hereby found and determined that all formal actions of this Council concerning and relating to the passage of this ordinance were adopted in an open meeting of this Council, and that all deliberations of this Council and of any of its committees that resulted in such formal action were in meetings open to the public, in compliance with all legal requirements including Section 121.22 of the Ohio Revised Code.

SECTION 6. That this ordinance is hereby declared to be an emergency measure necessary for the immediate preservation of the public peace, health, and safety of said city, and for the further reason that it is necessary to immediately update the city's cybersecurity policy; wherefore, this ordinance provided it receives an affirmative vote of two-thirds (2/3) of the members elected Council, shall take effect immediately upon its passage and approval by the Mayor; otherwise, it shall take effect and be in force from and after the earliest period allowed by law.

Passed: November 10th, 2025

Attest: _____
Clerk of Council

Submitted to the Mayor for approval on

November 10th, 2025

First Reading October 13, 2025*

Second Reading October 27th, 2025

Third Reading November 10th, 2025

* AMENDED on the floor from OR2025-50

_____
Council President – Presiding Officer

Approved: November 10th, 2025

_____
Mayor

Passed November 10th

Yes 4 No Ø

I, Sandra J. Fink, Clerk of Council of Wickliffe, Ohio, hereby certify the foregoing is a true copy of Ordinance No. 2025-50 AMENDED enacted by Council at its regular meeting on November 10, 2025.

CYBERSECURITY POLICY FOR THE CITY OF WICKLIFFE, OHIO

A. INTRODUCTION

The City of Wickliffe ("City") acknowledges the ever-changing landscape of the Internet and the importance of safeguarding public funds from Cybersecurity and Ransomware incidents. To that end, the City has adopted this Cybersecurity Policy to provide its Public Officials and Employees with expectations regarding a cybersecurity or ransomware incident.

B. DEFINITIONS

1. "*Cybersecurity incident*" means any of the following:
   (a) A substantial loss of confidentiality, integrity, or availability of the City's information system or network;
   (b) A serious impact on the safety and resiliency of City's operational systems and processes;
   (c) A disruption of City's ability to engage in business or industrial operations, or deliver goods or services;
   (d) Unauthorized access to City's system or network, or nonpublic information contained therein that is facilitated through or is caused by either:
      (i) a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or
      (ii) a supply chain compromise.
2. A "cybersecurity incident" does not include mere threats of disruption as extortion; events perpetrated in good faith in response to a request by the system owner or operator; or lawfully authorized activity of a United States, state, local, tribal, or territorial government entity.
3. "*Ransomware incident*" means a malicious "cybersecurity incident" in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable the City's information technology systems or data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

C. IMPLEMENTATION

1. Upon the City experiencing a cybersecurity incident or ransomware incident, the City Council shall notify Lake County **Information Technology Department** and both of the following:
   (a) ~~The Executive Director of the Division of Homeland Security within the Department of Public Safety, in a manner prescribed by the Executive Director, as soon as possible but not later than seven days after the City discovers the incident;~~
   ~~If this is an emergency, please dial 911. Report a Cyber Incident:~~ The Ohio Cyber Integration Center at Email: OCIC@dps.ohio.gov or Phone 614-387-1089. ~~If you are a public, local government entity, or a critical infrastructure operator experiencing a cyber incident and would like to request assistance from the state, including initiating aid from the Ohio Cyber Reserve, please us the contact information above to initiate a response;~~ and;
   (b) The Auditor of the State of Ohio, in a manner prescribed by the Auditor, as soon as possible but not later than thirty days after the City discovers the incident.
2. The City shall not pay or otherwise comply with a ransom demand regarding a "ransomware incident" unless the City Council formally approves such payment or compliance with the ransom demand in a resolution or ordinance that specifically states why the payment or compliance with the ransom demand is in the best interest of the City.
3. Pursuant to Ohio Revised Code Section § 9.64, any records, documents, or reports related to the Cybersecurity Policy and framework, as further detailed below, and any reports of a

cybersecurity incident or ransomware incident *are not public records* under Section 149.43 of the Revised Code. Furthermore, all records identifying cybersecurity-related software, hardware, goods, and services, that are being considered for procurement, have been procured, or are being used by the City, including the vendor name, product name, project name, or project description, are security records pursuant to Ohio Revised Code § 149.433.

D. DELEGATION

1. The City Council hereby adopts this Cybersecurity Policy to safeguard the City's data, information technology, and information technology resources to ensure availability, confidentiality and integrity. The City Council hereby delegates the Lake County IT Department/staff, the City of Wickliffe's Police Department's IT staff, or their designee with the responsibility to ensure the Cybersecurity Policy is, at all times, consistent with generally accepted best practices for cybersecurity, such as the National Institute of Standards and Technology Cybersecurity Framework and the Center for Internet Security Cybersecurity Best Practices. The County, the City's IT Professionals, or their designee shall ensure that the Cybersecurity Policy includes accepted best practices; and that Lake County:

   (a) Identifies and addresses the critical functions and cybersecurity risks of the City;
   (b) Identifies the potential impacts of a cybersecurity breach;
   (c) Specifies mechanisms to detect potential threats and cybersecurity events;
   (d) Specifies procedures for the City to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents;
   (e) Establishes procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident; and
   (f) Establishes cybersecurity training requirements for all City employees, of which the frequency, duration, and detail of such training shall correspond to the specific duties for each employee. Annual cybersecurity training provided by the State or the Ohio Persistent Cyber Initiative Program of the Ohio Cyber Range Institute shall satisfy the cybersecurity training required by this policy.

2. The City shall require that the completion of training of all City employees pursuant to this policy shall be confirmed by an employee's immediate supervisor, with any provided certificate forwarded to the Chief, Mayor, or their designee.

ORDINANCE NO. 2025 – 50

AN ORDINANCE ADOPTING A CYBERSECURITY POLICY FOR THE CITY OF WICKLIFFE, OHIO; AND DECLARING AN EMERGENCY

WHEREAS, the City of Wickliffe recognizes the importance of establishing clear and consistent policies to guide municipal operations; and

WHEREAS, the Cybersecurity Policy has been reviewed and recommended by the Law Director of the City of Wickliffe, Ohio; and

WHEREAS, City Council finds it to be in the best interest of the City to formally adopt and implement said policy to ensure transparency, consistency, and compliance with applicable laws as well as to safeguard public funds form cybersecurity and ransomware incidents;

NOW, THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF WICKLIFFE, COUNTY OF LAKE, AND STATE OF OHIO:

SECTION 1. The City of Wickliffe hereby adopts the document entitled "Cybersecurity Policy for the City of Wickliffe, Ohio", a copy of which is attached hereto and made a part hereof as *Exhibit A*.

SECTION 2. This policy shall apply to all [employees, departments, contractors, etc.] of the City of Wickliffe and shall take effect immediately upon passage unless otherwise stated in the policy document.

SECTION 3. The Mayor, or their designee, is authorized to take any necessary administrative actions to implement and enforce this policy.

SECTION 4. If any section, clause, or provision of this ordinance is declared invalid by a court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of this ordinance.

SECTION 5. That it is hereby found and determined that all formal actions of this Council concerning and relating to the passage of this ordinance were adopted in an open meeting of this Council, and that all deliberations of this Council and of any of its committees that resulted in such formal action were in meetings open to the public, in compliance with all legal requirements including Section 121.22 of the Ohio Revised Code.

SECTION 6. That this ordinance is hereby declared to be an emergency measure necessary for the immediate preservation of the public peace, health, and safety of said city, and for the further reason that it is necessary to immediately update the city's cybersecurity policy; wherefore, this ordinance provided it receives an affirmative vote of two-thirds (2/3) of the members elected Council, shall take effect immediately upon its passage and approval by the Mayor; otherwise, it shall take effect and be in force from and after the earliest period allowed by law.

Passed: _____, 2025

_____
Council President – Presiding Officer

Attest: _____
Clerk of Council

Approved: _____, 2025

Submitted to the Mayor for approval on

_____, 2025

_____
Mayor

First Reading October 15th, 2025

Passed _____

Second Reading See OR 2025-50 Amended.

Yes____ No____

Third Reading _____

CYBERSECURITY POLICY FOR THE CITY OF WICKLIFFE, OHIO

A. INTRODUCTION

The City of Wickliffe ("City") acknowledges the ever-changing landscape of the Internet and the importance of safeguarding public funds from Cybersecurity and Ransomware incidents. To that end, the City has adopted this Cybersecurity Policy to provide its Public Officials and Employees with expectations regarding a cybersecurity or ransomware incident.

B. DEFINITIONS

1. "*Cybersecurity incident*" means any of the following:
   (a) A substantial loss of confidentiality, integrity, or availability of the City's information system or network;
   (b) A serious impact on the safety and resiliency of City's operational systems and processes;
   (c) A disruption of City's ability to engage in business or industrial operations, or deliver goods or services;
   (d) Unauthorized access to City's system or network, or nonpublic information contained therein that is facilitated through or is caused by either:
      (i) a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or
      (ii) a supply chain compromise.
2. A "cybersecurity incident" does not include mere threats of disruption as extortion; events perpetrated in good faith in response to a request by the system owner or operator; or lawfully authorized activity of a United States, state, local, tribal, or territorial government entity.
3. "*Ransomware incident*" means a malicious "cybersecurity incident" in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable the City's information technology systems or data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

C. IMPLEMENTATION

1. Upon the City experiencing a cybersecurity incident or ransomware incident, the City Council shall notify Lake County and both of the following:
   (a) The Executive Director of the Division of Homeland Security within the Department of Public Safety, in a manner prescribed by the Executive Director, as soon as possible but not later than seven days after the City discovers the incident; and
   (b) The Auditor of the State of Ohio, in a manner prescribed by the Auditor, as soon as possible but not later than thirty days after the City discovers the incident.
2. The City shall not pay or otherwise comply with a ransom demand regarding a "ransomware incident" unless the City Council formally approves such payment or compliance with the ransom demand in a resolution or ordinance that specifically states why the payment or compliance with the ransom demand is in the best interest of the City.
3. Pursuant to Ohio Revised Code Section § 9.64, any records, documents, or reports related to the Cybersecurity Policy and framework, as further detailed below, and any reports of a cybersecurity incident or ransomware incident *are not public records* under Section 149.43 of the Revised Code. Furthermore, all records identifying cybersecurity-related software, hardware, goods, and services, that are being considered for procurement, have been procured, or are being used by the City, including the vendor name, product name, project name, or project description, are security records pursuant to Ohio Revised Code § 149.433.

D. DELEGATION

1. The City Council hereby adopts this Cybersecurity Policy to safeguard the City's data, information technology, and information technology resources to ensure availability, confidentiality and integrity. The City Council hereby delegates the Lake County IT Department/staff, the City of Wickliffe's Police Department's IT staff, or their designee with the responsibility to ensure the Cybersecurity Policy is, at all times, consistent with generally accepted best practices for cybersecurity, such as the National Institute of Standards and Technology Cybersecurity Framework and the Center for Internet Security Cybersecurity Best Practices. The County, the City's IT Professionals, or their designee shall ensure that the Cybersecurity Policy includes accepted best practices; and that Lake County:

   (a) Identifies and addresses the critical functions and cybersecurity risks of the City;
   (b) Identifies the potential impacts of a cybersecurity breach;
   (c) Specifies mechanisms to detect potential threats and cybersecurity events;
   (d) Specifies procedures for the City to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents;
   (e) Establishes procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident; and
   (f) Establishes cybersecurity training requirements for all City employees, of which the frequency, duration, and detail of such training shall correspond to the specific duties for each employee. Annual cybersecurity training provided by the State or the Ohio Persistent Cyber Initiative Program of the Ohio Cyber Range Institute shall satisfy the cybersecurity training required by this policy.

2. The City shall require that the completion of training of all City employees pursuant to this policy shall be confirmed by an employee's immediate supervisor, with any provided certificate forwarded to the Chief, Mayor, or their designee.