City of Waukesha
Change Management Policy

I. **Purpose.** This City of Waukesha Change Management Policy is necessary for ensuring confidentiality, integrity, and availability of the City of Waukesha production environment by controlling changes to all City of Waukesha servers, applications, network infrastructure, and workstations.

II. **Definitions.** For purposes of this Policy, capitalized terms have the following meanings:

A. **Production Environment:** An environment where functionality and availability must be ensured for the completion of day-to-day activities.

B. **Change Management:** The set of processes that allow changes to be introduced into the production environment in a controlled fashion that minimizes disruption and maximizes efficiency.

C. **Normal Change:** All changes that are not Standard or Emergency.

D. **Standard Change:** Tasks that are well known, documented, and proven. The risk is low and well understood.

E. **Emergency Change:** A change to resolve a current, or imminent threat to the production environment.

III. **Applicability.** This policy applies to any change to the City's production network.

IV. **Rules of Use.** The following rules must be followed by all Users:

A. All changes to the City of Waukesha's production environment shall get formal approval and sign-off using an electronic change management system.

B. Change requests will have an appropriate communication plan, and appropriate and reasonable back-out plans attached. If a back-out plan is not feasible, note this on the change request.

C. For major systems, the vendor will either perform the change or work closely with IT staff during the change.

D. All Normal change requests should be submitted for review by the IT department 7 days prior to the change.

E. All Standard change requests should be presented during the weekly change management meeting, with a minimum of 24 hours prior to the change.

F. If an urgent or emergency change is required, targeted e-mails shall notify affected users with as much forewarning as possible given the situation.

G. One may complete change approvals after-the-fact in an emergency requiring immediate action - when a system or parts of a system is down and repair is critical for business operations. Prior notification of emergency changes though not required, an

incident summary shall communicate to users the change and to report any adverse effects immediately.

H. When making changes, follow appropriate separation of duties whenever possible. In certain circumstances, it may be impossible to keep this separation – in those circumstances then note any potential conflict on the change request form.

I. Changes to test/development environments do not need approval through the change management policy, but track significant changes as part of project documentation in order to replicate in the production rollout.

J. Document required user testing of the change. The extent of testing should be commensurate with the complexity or impact of the change.

K. IT management shall review periodically any system-generated logs of program and data changes to ensure unauthorized changes have not to production.

V. **Security.** Every Change has the potential to compromise confidentiality, integrity, availability, and safety. The following rules must be followed by all Users:

A. The Rule of Least Privilege: The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

B. Separation of Duties: The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

C. Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems.

VI. **Standards.** The following standards support this policy**:**

A. IT Infrastructure Library (ITIL)

B. National Institute of Standards and Technology (NIST)Cyber Security Framework

C. Control Objectives for Information and related Technology (COBIT)

VII. **Regulatory Requirements.** The following regulatory requirements support this policy:

A. Criminal Justice Information Services (CJIS) Security Policy (Version 5.9)

B. America’s Water Infrastructure Act of 2018

VIII. **Related Policies and Documents.** The following documents are significantly related:

A. Vulnerability Management Plan

B. PCI DSS Cybersecurity Policy & Standards

IX. **Penalties for Violations.** Violations of these rules will subject the User to discipline, up to and including termination, as provided in Human Resources Policy G-3.

Passed this xx day of [MONTH] 202X.
Approved this xx day of [MONTH] 202X.

_____
Mayor

ATTEST:

_____
City Clerk