City of Milwaukee

Acceptable Use Policy

NIST Reference:	Implementation Date :	Revision Number :
AC – Access Control	**Pending Formal Adoption**	0.0

PURPOSE :

Information resources are strategic assets of the City of Milwaukee and must be treated and managed as valuable resources. The purpose of this policy is to do the following:

- Establish minimum appropriate and acceptable requirements regarding the use of information resources connected to the City Network.
- Comply with applicable state law and other rules and regulations regarding the management of information resources.
- Educate individuals who may use information resources with respect to their responsibilities associated with computer resource use.
- Establish a process to ensure that users acknowledge and agree to abide by the rules of behavior before gaining access to information resources connected to the City Network

SCOPE:

The City of Milwaukee Information Security Policies require departments and agencies to adopt an acceptable use policy for the use of the City Network and the Internet.

GENERAL POLICY:

This Acceptable Use Policy, sets out the minimum requirements for the use of City of Milwaukee resources. Agencies or departments may adopt more stringent policies. Exceptions to the minimum requirements in this policy template must be approved in writing by the Chief Information Officer. This Acceptable Use Policy states:

1. Users may not connect personal devices to the City Network without express written permission from agency or department management.
2. Personally owned “smart” devices may not be connected to the City Network. “Smart” devices, commonly referred to as the “Internet of Things,” include smart thermostats, smart appliances, or wearable technologies.
3. All devices connected to the City Network must have updated malware/anti-virus protection.
4. Participation in the Emergency Notification System is required for all City of Milwaukee employees. All individuals with wireless communication devices paid for in whole or part by the City of Milwaukee must participate in the emergency text message system.
5. Users must not attempt to access any data, documents, email correspondence, and programs contained on systems for which they do not have authorization.
6. Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization.

7. Users must not share their account(s), passwords or similar information or devices used for identification and authorization purposes.
8. Users must not make unauthorized copies of copyrighted or City-owned software.
9. Users may not download, install or distribute software to City-owned devices unless it has been approved by agency or department management.
10. Users must ensure all files downloaded from an external source to the City Network or any device connected to the City Network, including, compact discs (CD), USB flash drives, or any other electronic medium, is scanned for malicious software such as viruses, Trojan horses, worms or other malicious code.
11. Users must ensure that the transmission or handling of personally identifiable information (PII) or other sensitive data is encrypted or has adequate protection.
12. Users must not download City data to personally owned devices unless approved by agency or department management.
13. Users must comply with the City's Data Retention Schedules.
14. Users must not purposely engage in activity that is illegal according to local, state or federal law, or activity that may harass, threaten or abuse others, or intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene.
15. Users must not engage in activity that may degrade the performance of information resources, deprive an authorized user access to resources, obtain extra resources beyond those allocated, or circumvent information security measures.
16. Information technology resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, personal business ventures, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.
17. Access to the Internet from City-owned, home based, devices must adhere to all acceptable use policies. Employees must not allow family members or other non-employees to access nonpublic accessible information systems.
18. The City of Milwaukee offers a Guest network available in select locations for public access. Information being sent or received over the Guest wireless network should be considered non confidential and should never be used to conduct City of Milwaukee business. The City of Milwaukee offers secured connection solutions for business use.
19. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of information.
20. Users must report any incidents of possible misuse or violation of the Acceptable Use Policy.
21. Users should have no expectation of privacy with respect to the City's telecommunications, networking or information processing systems (including, without limitation, files, e-mail messages and voice messages) and that user activity and any files or messages on or using any of those systems may be monitored at any time without notice.

ENFORCEMENT

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

NIST Reference:	Implementation Date :	Revision Number :
AC – Access Control	**Pending Formal Adoption**	0.0

REVISION HISTORY:

Revision	*Date*	*Changes*
0.0	July 8, 2019	Draft