



Information Management Services Division

Department of Administrative Services

Title: Acceptable Use Policy
Approval: Chief Information Officer

Issue Date: 09/01/2013
Supersedes: Use of Technologies
Policy 12/99

Definitions:	• County: Milwaukee County Government • Information Systems and/or Technologies: A combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making in an organization. All components used by Milwaukee County Government to carry out some or all of its planned tasks. Included are: ○ <i>Hardware</i> - All hardware technology components, all of which work together to accept, process, and display data and information. ○ <i>Software</i> - The programs that allow the hardware to process the data. ○ <i>Databases</i> - The gathering of associated files or tables containing related data. ○ <i>Networks</i> - The connecting systems that allows diverse computers to distribute resources. ○ <i>Procedures</i> - The commands for combining the components above to process information and produce the preferred output. • Users: the County of Milwaukee, its departments, commissions, boards, offices, and agencies, and all officers, employees, temporary employees, interns, vendors, consultants, contractors and agents thereof.
Purpose:	This Policy outlines the acceptable protection and use of information and information technology within Milwaukee County Government (the "County"). These rules are in place to protect the employee and the County, because inappropriate and/or unacceptable use exposes the employee and the County to risks that can compromise the confidentiality, integrity and availability of information. The objectives of this policy are to: • increase awareness of computer security among Users; • define ethical and lawful behavior by Users and providers of information; • detail the consequences of inappropriate or unacceptable use of the County's data and/or resources; • provide a guideline for protecting County data and/or information resources from theft, loss, damage and unauthorized access or alteration; Increase awareness of proper protocol regarding the County's confidential data, material and information. Confidential material, data and information refers to information that is not generally known outside the County and belongs to, is used by, or is in the possession of the County, including without limitation information concerning financial reports and analysis, cost data and cost structures, strategic plans and other confidential technical or business information and data as well as any background data that provides the basis



Information Management Services Division

Department of Administrative Services

	for any of the foregoing plans and programs.
Principles:	All information systems equipment provided by the County assists Users in the performance of their work functions and remains the sole property of the County. Any information created by the User in the scope of or related to their employment also remains the property of the County and must not be removed, copied or shared without express permission, except to assist the User in the performance of his or her work at County,. Users must use County information systems and communications facilities responsibly, lawfully, consistently with their duties, and with respect for their colleagues and customers. Users acknowledge and agree that: • electronically stored documents and e-mails are County property and may be subject to production in a legal action or open records request. • limited personal use is at the absolute discretion of the County and no User may expect or claim such personal use as a right or expect such use to be private. This use is subject to the procedures and rules established by this policy. The County may monitor and disclose electronically stored information to ensure compliance with this policy, to comply with law enforcement requests, to complete an investigation, to defend the County in legal proceedings, to comply with open records requests and for legitimate business reasons, consistent with the law. • they represent the County in their interactions with the outside world. • they are required to comply with any notices regarding the retention or destruction of electronically stored information, including e-mails, electronic calendars and other documents
Scope:	This document records the County's policy regarding: • The correct and proper (i.e., acceptable) usage by Users of the County's data and computer systems (including video conferencing equipment, webcams and other electronic devices, and digital media and storage devices) but excluding telephones; • Users' access to and use of Internet access provided by the County; and • Electronic information, including data and e-mail messages, sent and received by Users via County e-mail and other communication systems. This Acceptable Use Policy applies to the County of Milwaukee, its departments, commissions, boards, offices, and agencies, and all officers, employees, temporary employees, interns, vendors, consultants, contractors and agents thereof--collectively referred to as —User(s).
Accountability:	The County computer systems and all information thereon are critical government assets and are not to be mistreated or abused by any User. A User who contravenes the terms and conditions of this policy acknowledges that he or she will be acting outside of the course and scope of his or her employment, or, if a non-employee, his or her obligations to the County.



Information Management Services Division

Department of Administrative Services

	Failure to comply with this policy may result in disciplinary action against the User up to and including termination of employment of employees or termination of the engagement of non-employee Users. With regard to a contract worker or non-employee User of the County's computer system, such User will be obliged to acknowledge the policy and refrain from any contravention of this policy.
Policy/Procedure:	1. Information Technology a. Access i. Only authorized Users may access the County computer network or systems by means made available by the County. ii. Users may access County computer systems, e-mail and Internet facilities only by means of their authorized usernames and passwords. Users must not knowingly share or allow the use of their username outside of the County and/or share their password with anyone internal or external to the County. Users are accountable for all work saved or retrieved, messages sent or received, or transactions carried out under their usernames and passwords. iii. Users must not access, download or distribute any material that could be deemed pornographic, racist, sexist or otherwise offensive or in violation of County policies, state/federal laws. The display of any such image or document on a County system is expressly prohibited and such images or documents may not be archived, stored, distributed, edited or recorded on the County's network or computer resources. iv. Users of County networks or computer resources must not seek to gain access to restricted areas of the network or access/try to access, copy, alter or delete the data of any other User without authorization. b. Inappropriate Network/Software Activity i. Users of County computing resources must not attempt to probe, scan, or breach the security or authentication measures of a system or network either internally or externally using either County resources or other tools, software or code that enables a User to circumvent a computer system's security. ii. Users of County networks or computer resources must not knowingly disable or overload any computer network, or circumvent any system intended to protect the security of another User.



Information Management Services Division

Department of Administrative Services

	iii. Users of County networks or computing resources must not knowingly propagate any virus, worm, Trojan horse, trap-door program, or similar code. If such virus, worm, Trojan horse, trap-door program, similar code, or other security incident is discovered by a User, he/she must immediately disconnect from all networks, cease using the system and immediately report the discovery to the Service Desk. iv. Only software that County owns or has a license to install shall be installed on County computers. Users must not install unauthorized software. Unauthorized software is software that is not installed originally on the computer or later by the Information Management Services Division, , not licensed by the County for business use, and/or not supported by County computing resources. Users may apply for an exception to this policy by providing adequate business justification with management approval and proof of proper licensing to the Information Security department for consideration and evaluation of risk. c. Data and Physical Security Concerns i. Users must store all business-related files in County designated storage locations where they can be backed up. Data stored on removable/mobile storage devices like flash drives or CDs should be restricted to information that is not deemed private, confidential or subject to Open Records requests. Personal files are not private and the County may read and disclose those files to ensure compliance with this policy, to comply with law enforcement requests, to complete an investigation, to defend the County in legal proceedings, and for other legitimate business reasons consistent with the law. Therefore, the practice of storing personal files on local workstations is strongly discouraged and abuse could result in discipline at management discretion. At no time should personal files reside on County servers (on or off premise). Again, personal files are not private and the County may read and disclose those files to ensure compliance with this policy, to comply with law enforcement requests, to complete an investigation, to defend the County in legal proceedings, and for other legitimate business reasons consistent with the law. ii. Users of County computing resources must take adequate steps to protect the physical security of the computing resources within their possession by ensuring portable devices are securely stored when not in use and workstations are locked when left
--	--



Information Management Services Division

Department of Administrative Services

	unattended. Any theft or loss of IT equipment must immediately be reported to the Service Desk. iii. Users of County networks or computing resources must ensure that all data that may be required to be retained by applicable laws or regulations or by the County's record retention policies are retained and stored in compliance with such laws, regulations and policies. This includes recordings of audio or video. d. Information Technology Security and Passwords i. Users must follow password standards to prevent unauthorized access to County computer systems and data. Users must not share fixed passwords with anyone, including managers and co-workers. Users must not store fixed passwords in any computer files, such as logon scripts or computer programs, unless the passwords have been encrypted with authorized encryption software. All fixed passwords set by default by the hardware or software vendor must be changed before the involved system can be used for County business activities. ii. All employees must ensure County-provided hand-held mobile devices (such as BlackBerrys, smartphones, or tablets) are protected with a password or a passcode. iii. Employees must comply with applicable laws and ordinances relating to mobile device usage while driving, and Users are strongly discouraged from using mobile devices while operating a vehicle even where it is legal to do so. Employees must act responsibly and safely while using any hand-held mobile device. Employees who may use mobile devices while operating a vehicle are obligated to familiarize themselves with relevant state and local laws. If an employee does not know whether a particular use is allowed, he or she must refrain from that use. iv. Mobile devices, including laptops, tablets and smart phones, must be adequately secured and not left in places where they are visible to passersby. Users also must secure their laptops and other mobile devices in locked cabinets if they decide not to take them in the evening or for long periods of time. Sensitive data stored on these devices could be compromised if they are stolen or lost. e. Remote Use i. County computing resources should not be accessed by non-Users in remote situations unless County personnel are closely monitoring such access.
--	---



Information Management Services Division

Department of Administrative Services

	ii. Users must ensure that confidential information is not inadvertently viewed by third parties. iii. Users must comply with the Mobility Devices Procurement & Usage Guideline. iv. Remote use of County systems must comply with all other aspects of this document. 2. Electronic Mail and Messaging Systems a. Business Messaging i. Users must take particular care when using e-mail as a means of communication because, although potentially informal in nature, email communications may be subject to production in a legal action or open records request. ii. Users may access approved instant messaging services only for informal business communication similar to a quick phone call or quick in-person verbal communication, unless the content of the messages is subject to an instruction to preserve records and electronically stored information. Users may not send or receive file attachments via instant messaging services. Users must only communicate with known trusted correspondents via instant messaging, and communication with anyone not in the User's contact/buddy list should be blocked. Instant messages should not be used to transfer or record any substantive government information because instant messages are not stored or saved. Instant messages should not be used to convey non-work-related information. iii. Users must not send or forward e-mail messages, e-mail attachments or instant messages, which could be construed as defamatory, discriminatory, harassing or otherwise offensive. iv. Users must not send sensitive or confidential information over the Internet without adequate protection securing the information's confidentiality. v. Users of County's e-mail and messaging systems must not knowingly distribute or forward hoax virus warnings, chain letters, jokes, political commentaries, or similar unsolicited e-mail of any kind. vi. Users must not access any other User's in-box without explicit authorization from that User (e.g. through Outlook delegates) or permission from Manager, Enterprise Security or Legal.
--	--



Information Management Services Division

Department of Administrative Services

	vii. Users must not send any e-mail purporting to come from another User without explicit authorization from that User (e.g., through Outlook delegates). b. Personal Messaging i. The County's e-mail facilities are provided principally for business purposes. While it is acceptable for Users to occasionally use email for personal purposes, abuse of this privilege could lead to disciplinary action at the discretion of the manager. This limited personal use is at the absolute discretion of the County and no User may expect or claim such personal use as a right or expect such use to be private. This use is subject to the procedures and rules set out in this policy. The County may monitor and disclose e-mails to ensure compliance with this policy, to comply with law enforcement requests, to complete an investigation, to defend the County in legal proceedings, and for other legitimate business reasons, consistent with the law. ii. Under no circumstances may the County's facilities be used by employees in connection with solicitations for outside organizations, political or religious causes, or with the operation or management of any business other than that of the County. iii. Users must ensure that their personal e-mail and messaging use: 1. does not interfere with the performance of their duties; 2. does not cause unwarranted expense or liability to be incurred by the County; 3. is lawful and complies with this policy; and 4. is not excessive. iv. Any communication using the County's electronic facilities is not private, may be reviewed and disclosed by the County for the reasons listed in the policy, is retained by the County subject to applicable retention guidelines, and may be recoverable from the User's computer. As such, Users should carefully consider whether to use County systems to access personally confidential information such as personal e-mail accounts, personal online accounts, etc. Doing so through the County's system is not confidential and all such information is viewable by County and subject to disclosure for the reasons identified in this policy. v. Any personal use of the County's electronic facilities signifies a User's consent to this policy's application to the personal use. vi. Employees may not send "system-wide" or "all user" messages or
--	---



Information Management Services Division

Department of Administrative Services

	blasts due to their disruptive effect. 3. Internet and Intranet a. Business Internet Access i. When visiting an Internet site, information identifying a User's PC may be logged (i.e. cookies, temp files). Therefore any activity in which Users engage may reflect upon the County. ii. Users must not access inappropriate websites, blogs, discussion forums or chat rooms, which have content that could be construed as defamatory, harassing or otherwise offensive or in violation of County policies prohibiting harassment. iii. Users must always exercise caution when using a County e-mail address to join networking sites. While such use may be appropriate for some (e.g. Linked-In), for others this may not be the case. Remember, Users' County e-mail addresses are provided for work purposes. iv. Whenever Users access a web site, they must always comply with the terms and conditions governing its use. v. The County routinely blocks access to Internet sites that are deemed to be inappropriate or to pose an information security threat to the County. This includes Internet webmail sites since they can be used to leak sensitive data. Any attempts to access blocked Internet sites are monitored and recorded. If a User must, for business reasons, access an Internet site that is prohibited by the County, the User must obtain explicit and written permission from his/her County Department head requesting limited access to that particular site for the stated business purpose(s). vi. Users are prohibited from posting confidential or sensitive information to the Internet (including, but not limited to, usernames, passwords, security codes or server-specific information, or information that could assist third parties in gaining unauthorized access to the County computer system). vii. Users must not send any confidential or sensitive information (including, but not limited to, credit card numbers, telephone calling card numbers, fixed passwords, or customer account numbers) through the Internet unless the connection is encrypted (i.e. https). viii. Downloading, copying, possessing and distributing material from the Internet risks infringement of copyright or of other
--	--



Information Management Services Division

Department of Administrative Services

	intellectual property rights. Users must not download software from the Internet unless specifically authorized to do so by Information Management Service Division. Users of County networks or computing resources must not download or distribute pirated software or data. ix. The County may monitor and disclose Internet usage to ensure compliance with this policy, to comply with law enforcement requests, to complete an investigation, to defend the County in legal proceedings, and for other legitimate business reasons, consistent with the law. As such, Users have no reasonable expectation of privacy in Internet activity or other communications via County computer systems/technologies/networks. b. Personal Internet Access i. The County recognizes the need for Users to perform some personal tasks during working hours, e.g. for Internet banking or on-line shopping, and this is permitted subject to the same rules as are set forth for personal e-mail use in Sections 2(b) of this policy. ii. If acting in a personal capacity, you should be mindful of your online conduct and its potential impact, especially if you have listed County as your employer. Even if you have not mentioned County, in an ever-connected world your association with the government may be considered public knowledge. iii. Think carefully about the amount and type of information you reveal in your online profiles. Do not reveal details that should not be public. Consider restricting access to your profile using the site's privacy settings, where available. iv. Users are expressly prohibited from using web logs (or blogs) to disclose or discuss any confidential or proprietary County information. Users must not use the County trademarks or logos no matter when or where web logs are used. The use of web logs unrelated to County business from County devices and/or during work hours is expressly prohibited. v. Music and video files (e.g. MP3, MP4), unless specifically authorized for business purposes, are not allowed on any County servers because of the potential copyright and legal liability over where those files originated. All music files will be deleted from County servers when found. Streaming audio (e.g., Internet radio) and video, unless specifically authorized for business purposes, is not allowed on any County resources because of the
--	--



Information Management Services Division

Department of Administrative Services

	significant negative impact such streaming has on system capacity and User productivity. vi. Subject to this policy, Users may download a reasonable amount of personal documents or images not related to County business but must not store these images or files on County workstations or servers. Personal files are not private and the County may read and disclose those files to ensure compliance with this policy, to comply with law enforcement requests, to complete an investigation, to defend the County in legal proceedings, and for other legitimate business reasons consistent with the law. c. Social Media or Networking Sites i. With any social media interaction, Users must be mindful of, and clear about, the capacity in which they are participating. Only trained County spokespersons should make statements on behalf of our businesses or brands. If you are not a designated and approved County spokesperson in the traditional media, you may not act as one in the social media space. ii. Information posted on social networking sites can have far-reaching consequences for Users and County. All expressions of fact, intention and opinion may bind the User and/or County and can be produced in court in the same way as other kinds of written statements. iii. Interactions on social media or networking sites must comply with all County policies. 4. General Security a. Users who maintain "isolated" data such as safe combinations, alarm codes, domain name registry passwords, administrative passwords, off-site storage access codes, etc., must contact the Milwaukee County Security Officer to ensure that duplicate copies of the information are securely maintained. b. Users must not take any action that is offensive to or inconsiderate of individuals or entities that are users or subjects of information resources (e.g., use of webcams, video conferencing equipment, recording device or microphones for non-business purposes). 5. Communications a. The County is ultimately responsible for all government communications and may monitor a User's electronic communications for reasons that include:
--	---



Information Management Services Division
Department of Administrative Services

	• Ensuring compliance with this policy; • Complying with law enforcement requests; • Completing an investigation; • Defending the County in legal proceedings, and • Other legitimate business reasons, such as providing evidence of business transactions; complying with any legal obligation, ethical code or best practice; preventing, detecting or investigating unauthorized use of County’s communications systems or criminal activities; and maintaining the effective operation of the County’s communication systems consistent with the law. b. Sometimes it is necessary for the County to access a User’s business communications during the User’s absence, such as when the User is away due to illness or leave. Unless the User’s mailbox settings are such that the individuals who need to do this already have permission to view their Inbox, the County will access the communications to do so with the permission of the Manager, Security or Corporation Counsel. c. In certain circumstances the County may, subject to compliance with any legal requirements, access personal e-mail sent or stored on County e-mail systems when it is already stored in County storage media. Such circumstances include those reasons otherwise outlined in this policy, situations when the County has reasonable suspicion that such access may reveal evidence of unlawful activity, violation of County policies, dereliction of job duties, instances when there may be a breach of a contract with the County, or when the County is otherwise obligated by law to do so.
	Milwaukee County Government Security Department The Milwaukee County Security Department is responsible for establishing and publishing policies and standards, providing advice and guidance, monitoring compliance, and coordinating the effort required for attaining security objectives. The Chief Information Officer or appointed delegate will report to the County’s Board on major incidents or threats, which could affect the continued operation of IT systems. Information Owners The County is the sole owner of all its data and information assets. For



Information Management Services Division

Department of Administrative Services

	responsibility purposes all data will have a designated 'Information Owner.' Owners are responsible for specifying measures to protect their information assets. Management responsibilities Heads of Agencies/Departments are responsible for ensuring that best security practices are implemented and maintained within their area of responsibility by: • ensuring that Users know what is expected of them and that the Users act in a responsible way to protect the County's data and information systems; • ensuring that standards and procedures are followed at all times; • maintaining an appreciation of the risks associated with the loss of confidentiality, integrity or availability of information and ensuring that where adequate standards and procedures are missing, an appropriate person is notified for action; and • setting a good example to Users by taking the lead in applying good security principles to their own work.
Contact:	CIO and Director of Information Management Services Division.