Online Cyber Security Awareness Training required by 06/30

Hackers and international conflict have made computer security awareness a high priority in every organization including the public sector. Employees play an important role in keeping Kent County's information technology infrastructure secure.

The human element makes a significant difference in the success of any cybersecurity program. Unfortunately, there is no single technology or user behavior that will completely protect you or the organization from cyber incidents. Keeping the organization safe requires developing layers of both technical and human defenses. Training that focuses on the human element of protecting information will help users recognize and reduce the risk of a cybersecurity breach.

As a result, the County Administrator has determined that each County employee must complete web-based MANDATORY Data Privacy & Information Security/Cyber Security Awareness training by June 30, 2022. As a general cybersecurity training course, some specific content may apply to corporate or international businesses, rather than the public sector. More specific content may be offered in future annual training sessions on this topic.

Kent County uses the **Zywave Learning Management system** for most web-based training. The system was introduced in 2020 for sexual harassment prevention training and thereafter for new hires.

Employees will soon receive an email from the Personnel Office welcoming employees to the **Zywave Learning Management system** or an email advising that a new training course has been assigned. First time users will need to set up an account per the directions included in the email. If you do not have regular access to a computer, see your supervisor to arrange training or contact the Personnel Office to schedule use of the I.T. training center.

Once an account and password are created, look for the training assignment and after setting up a block of training time (30 minutes) with your supervisor – complete the interactive web-based training process. The training course is designed not to allow viewers to minimize the session or ignore questions, and requires NEXT to be clicked often.

In addition to this mandatory training assignment, employees will regularly be assigned other online training seminars by the Personnel Office on various topics such as Ethics, Customer Service, Performance Improvement, etc.

Using your County email address (no personal emails) and Zywave log on, the 30-minute training will generate a certificate of completion. Employees may print the certificate for their own record. Please do not send a copy to the Personnel Office, since Zywave provides a report confirming completion by each individual employee.

The Kent County Computer Network Usage Policy is as follows:

Kent County Policy 4:

§ 4-13 **Computer network usage.**

[Adopted 9-12-2000 (P-81)]

This Policy establishes the guidelines for usage of all Kent County computer networks and computer network applications and includes Internet usage guidelines.

A. Policy compliance.

(1) Computer network and Internet systems, just as with other County resources, are for official use only. Use of Kent County networks and the Internet must be consistent with the goals of facilitating and disseminating knowledge, encouraging collaborative projects and resource sharing, aiding technical transfer to Kent County businesses, fostering innovation and competitiveness within Kent County, and building a broader infrastructure to support professional, work-related activities.

(2) Each department is responsible for the activities of its employees and for ensuring that its employees are familiar with this Policy.

B. Data processing standards.

(1) Use of County computers, e-mail, networks and the Internet subjects each user to monitoring. Transmitting inappropriate material over County networks or the Internet, including pornography, gambling material, documents containing religious or racially disparaging content, and illegally obtained copyrighted material, is a violation of this policy.

(2) The County e-mail system will be monitored and audited for inappropriate usage. Information shared using the e-mail system is not to be regarded as private or confidential. Mailing software files and chain mail is not authorized. Mass broadcast mailings to larger organizations should be limited to those needed for business purposes and may be made only with written approval from the sender's supervisor.

(3) Use of the Internet to further professional knowledge is authorized; however, accessing sites for entertainment, to further personal or commercial financial gain, or to participate in "chat rooms" is in violation of this Policy.

(4) Only licensed copies of software programs that are supported by the County Information Technology Office will be loaded and supported on County PC's and networks.

(5) Employees should not copy programs, zipped (compressed) files or other executable files into user or shared directories on the network.

(6) Users should monitor their own directories, ensuring that only current data is stored on the network. Old data (data that has not been accessed in six months) should be archived (by copying it to a floppy disk or CD) and deleted from the network, to enable efficient use of network storage space.

(7) Network backups will be performed nightly. Since any file open when the backups occur will not be copied to the backup, users should close all programs and log out of the network each night prior to leaving their workstation. This will enable the information stored on the networks to be successfully backed up in the nightly process. (Any data stored on the user's C drive will not be included in the nightly backup, as this information resides on the PC's hard drive only.)

(8) The networks will automatically prompt users to change their passwords each 30 days. Easily guessed passwords (such as initials, a child's name, birthdays) should not be used. Passwords should never be written or displayed on a workstation.

C. Privacy rights.

(1) Computer network systems (including e-mail) and Internet systems are the property of Kent County and are to be used for official County business only. Usage of these systems, and information shared using these systems, is not to be considered private or confidential in any manner or at any time.

(2) Computer network and Internet systems will be monitored and audited for inappropriate usage. If a user accidentally accesses questionable information using County-provided computer networks or the Internet, that user must immediately notify his or her supervisor of such access. Accidental access will be noted and will not be considered as a violation of this Policy, provided the proper notification is made immediately.

(3) Kent County reserves the right to remove unauthorized software and data from all County computer equipment without notice.

D. Acceptable uses. The following acceptable uses list includes ways that information on the County networks and the Internet may be used. This is not an inclusive list; each user should use his or her own discretion as to how to use the networks and the Internet for County business purposes, realizing that usage is monitored.

(1) To provide and facilitate communication with other County, state and federal agencies and business partners of Kent County agencies.

(2) To communicate and exchange professional development; to maintain or debate issues in a field of knowledge.

(3) To use for professional society, university association, government advisory, or standards activities related to the user's professional/vocational discipline.

(4) To use in applying for or administering grants or contracts for work-related applications.

(5) To use as a means of administrative communication or with activities in direct support of work-related functions.

(6) To announce products or services for use within the scope of work-related applications, but not for commercial advertising of any kind.

E. Principles of ethics. The following principles of ethics will apply to County computer networks and Internet usage:

(1) Users will not seek information on, obtain copies of, or modify files, data, or passwords belonging to other users.

(2) Users will not intentionally represent themselves as another user unless explicitly authorized to do so by that other user.

(3) Users will not violate copyright laws when using County computer networks and the Internet. Users will not load or use unlicensed software.

(4) Users will not intentionally develop programs that harass other users.

(5) Users will not invade a computer or computing system and/or damage or alter its software components.

F. Unacceptable uses. The following list identifies unacceptable uses of County computers, networks and the Internet. This list is intended as a guideline and is not inclusive.

(1) Transmitting or receiving inappropriate material. This includes sending or receiving pornographic or sexually provocative material, gambling material, documents containing religious or racially disparaging content, and illegally obtained copyrighted material.

(2) Illegal or malicious use. Use should be consistent with guiding ethical statements and accepted community standards. The County networks and the Internet may not be used in ways that violate applicable laws or regulations such as transmitting or soliciting threatening, obscene, or harassing materials. The County computer networks or the Internet may not be used to solicit information with the intent of using such information to cause personal harm or bodily injury.

(3) Changing the manner in which the networks communicate with each other or share information between users.

(4) Unsolicited commercial advertising.

(5) Use for recreational games, except in conjunction with a Kent County sponsored activity.

(6) Use for revenue-generating activities, unless related to Kent County business.

(7) Use for private or personal business activities.

(8) Displaying religious themes, comments or images.

(9) Distributing unsolicited advertising.

(10) Distributing computer worms or viruses.

(11) Gaining unauthorized entry to another machine.

(12) Attempting to circumvent County user authentication or security.

(13) Attempting to interfere with or deny service to any user or network.

(14) Forging e-mail header information.

(15) Sending unsolicited mail messages (spam or junk mail).

(16) Forwarding or posting "chain letters" of any type.

(17) Participating in Internet "chat rooms."

G. Remedial action. When the Information Technology Office (IT) learns of a possible inappropriate use, IT staff will immediately notify the Personnel Director and director of the department in which the inappropriate use occurred. In order to prevent further possible unauthorized activity, IT may temporarily disconnect an irresponsible user from the County network. Any determination of unacceptable usage serious enough to require disconnection will be promptly reported to the department director.

H. Violation of this Policy will be subject to disciplinary action up to and including termination and/or the suspension of use privileges (or access).

§ 4-13.1 **Social media use.**

[Adopted 6-14-2011 (P11-01)]

This Policy establishes provisions for the appropriate use of social media by employees, but is not intended to replace or substitute normal standards of good judgment and professional conduct.

A. Social media includes all forms of online computer applications, websites, tools, and platforms that enable communications between users. The specific types of social media change frequently but, as a general matter, include: (1) social networking sites such as Facebook, MySpace, Linkedln, etc. (2) blogs and microblogs such as Blogger,

Twitter, Wordpress, Tumblr, etc.; and (3) content-sharing sites such as You Tube, Flickr, Vimeo, Scribd, etc. Additionally, comments posted to a website or blog, and other user-generated content, are subject to the standards set forth in this Policy.

B. Employees are prohibited from engaging in, accessing, or otherwise using social media during working hours, unless authorized by their department head to so do as part of County-sponsored social media activities or job-related duties.

C. Misconduct via social media may result in disciplinary action under other County policies/ordinances. Employees should remain aware of the public nature of their online activities, and there should be no expectation of privacy with respect to content posted on the Internet.

D. Employees violating this policy shall be subject to disciplinary action, up to and including termination.

(posted 04/01/22)