VICTORIA COUNTY INFORMATION TECHNOLOGY AND CYBER SECURITY POLICY

Approved and adopted January 13th, 2020

I. Policy

A. This Policy governs the County of Victoria's technology resources operated by the by Elected Officials, employees, volunteers, vendors, contractors and all other authorized users. Technology includes, but is not limited to; desktops, laptops, mobile devices, networking equipment, networked devices, servers, software, electronic mail, phones, cellular phones, control systems, Internet, Intranet, and all other Enterprise electronic systems or devices.

B. The Information Technology Department (IT) shall establish and maintain specific rules and requirements relating to the safe and secure operation of all devices and the storage of data while connected to County resources. Adherence to these standards is a requirement for all persons utilizing County-owned devices, or storing and accessing data on County technology infrastructure. These standards shall be amended as necessary to remain current with various needs and risks, and are included in this policy by reference. Failure to comply with these rules and requirements shall be considered an improper use.

II. Definitions

A. For the purposes of this Policy and Procedure, the following definitions shall apply:

1. Improper Material - Pictures, posters, calendars, graffiti, objects, promotional materials, reading materials, or other materials that are racist, sexually suggestive, sexually/racially demeaning, pornographic, offensive, intimidating, harassing, disparaging, and/or hostile on the basis of age, disability, gender, national origin, race, color, religion, or any other legally protected characteristic.

2. IT Director - The Director of Information Technology of the County of Victoria or designee.

3. Department Head/Elected Official - The head of a department or office of the County of Victoria, or designee.

4. Employee - For the purpose of this policy, an employee is defined as an individual employed by the County on a full-time, part-time, seasonal, temporary or internship basis.

5. Mobile Device - Means a device intended to be portable, carried on one's person, or readily moved from location to location, such as smartphones, cell phones, radios, pagers, laptops, tablets, and others.

6. Authorized user - An authorized user is a current employee, contractor, vendor, or other party who has been granted lawful access by the IT Director to the County of Victoria network, applications, or services.

III. Procedures

A. Applicability

1. This policy shall apply to all County elected officials, employees, volunteers, vendors, contractors, and other authorized users as defined herein. Departments may develop departmental policies and procedures which provide greater direction to their employees, as long as that direction is consistent with, and does not override, this interdepartmental policy and procedure.

B. Authorized Use

1. The County electronic communications and technology resources are provided for the purpose of conducting County business. Occasional and Incidental personal usage is permitted, as long as such use is reasonable, prudent and does not interfere with the employee's job duties. The responsibility for the appropriate use of County electronic communication and technology resources ultimately rests with the individual employee, and standards developed per the Department Head/Elected Official.

2. Improper or Unauthorized use of the County's electronic communications and technology resources may result in disciplinary action, up to and including termination.

C. Privacy

1. No user accessing or using computers or telecommunications resources owned and/or operated by the County of Victoria can have any expectation of privacy. The County of Victoria reserves the right to monitor, intercept, archive, view, or distribute any communications and/or content transmitted over resources which it owns, leases, or operates subject to all applicable laws.

a) IT Staff may be required to access any and all material located on those resources.

b) Department Heads/Elected Officials may monitor their employees usage of the Internet and email, or may revoke an employee's access to the Internet and/or email by notifying the IT Director.

c) Authorized users must be aware that any digital record residing on a County-owned device may be subject to lawful open records requests. In addition, any data regarding County business stored on a personal device or file sharing service may be subject to lawful open records requests.

d) The department that an electronic device has been issued to is responsible for all costs associated with damage to or loss of the device. Lost, stolen or seized property must be reported to IT Director and Human Resources with 24 hours.

D. Resource Access Requirements

1. Work Product

a) No employee shall use the Internet, social media sites, or e-mail to present his or her own personal views, ideas, questions, or actions, as representing the positions or policies of the County unless doing so in an official capacity and authorized by the County Judge or his/her designee.

No employee shall use the Internet, social media sites, or e-mail to present his or her own personal views, ideas, questions, or actions, as representing the positions or policies of any particular office or department of Victoria County unless doing so in an official capacity and authorized by the Department Head/Elected Official or his/her designee.

b) Unless otherwise specified by contract, any work produced by a vendor, contractor, or other third party acting as an agent, consultant, or contractor to the County, is the property of the County, and employees shall take steps to ensure that such property is properly stored on County resources to prevent loss.

c) No employee shall use any County-owned equipment or resources in violation of any applicable law.

2. Identity

a) Each person authorized to access the County of Victoria's computer and network resources must do so using their unique user name (login name) assigned by the IT Department. The use of group accounts will be limited to only those circumstances approved by the IT Director. Employees shall not share their account information, or permit other employees to log in using their credentials excepting properly identified members of the IT department. Electronic communications authored by the employee must clearly originate from the user's unique account.

Department Heads/Elected Officials may review or access their employees computers and communications by contacting the IT Director.

3. New Employees

   a) It is the responsibility of each department to notify the IT Department at least three working days prior to the start date of any new employee or authorized user who needs access to the County's electronic resources, so that appropriate access can be provided on a timely basis.

   b) New employees must receive a copy of this policy during orientation, and acknowledge that they have read, and will adhere to, the contents of this document.

   c) It is the responsibility of each department to immediately notify the IT Department in the event of the termination, resignation, or retirement of any employee within their department who previously had access to County computers and/or network resources, so that such employee user accounts may be removed or set up for monitoring.

4. Remote Access to Resources – The County maintains various systems to permit users to access internal systems from non-secured locations, like the Internet. These services are intended to augment the productivity of employees.

   a) Employees must take extra precautions when accessing County resources from non-County devices. The use of a virus scanner is required.

   b) It is the responsibility of the employee using the remote access facility to ensure that unauthorized persons cannot utilize their account to gain access to County resources. Employees cannot provide their passwords to anyone, including family members.

   c) Users must understand that using their personal device or computer to access County resources may impose the possibility of open records access responsibility. This means you may be required to provide records from your personal device or submit your personal device to a search for either an open records or legal request if it accesses County systems.

   d) Unless specifically authorized by their Department Head/Elected Official, non-exempt employees may not use electronic devices to conduct County business outside their normal working hours.

5. Data Storage

   a) Employees should not store information exclusively on the local drive (C:, D:, etc.) of a Desktop PC, laptop or tablet. By storing the file outside of network or cloud storage provided by the County, the data is neither searchable nor backed up.

E. Internet - It is the policy of the County of Victoria to offer connectivity to the Internet for employees requiring its use as a part of their normally assigned duties. The purpose of this policy is not to discourage the use of the Internet, but to provide a uniform approach to the usage of this resource, to safeguard County interests in the use of the Internet, to meet all applicable laws, and to protect the assets attached to County networks from unauthorized access. The County of Victoria reserves the right to monitor all Internet usage on County-owned and County-connected devices including reviewing all sites that are viewed by the employee's browser and the amount of time spent at each site.

1. Appropriate Uses of Internet Resources - All County-owned Internet resources are intended to be used only in the pursuit of appropriate County business interests. Personal email messages or other non-County related usage of Internet resources should be held to a minimum, as with telephone calls.

2. Bringing Improper Material into the work environment or workplace, or producing, possessing, or distributing any Improper Material at work to read, display, view, or otherwise publicizing it in the work environment is prohibited.

3. No employee shall access any internet resources or connect to any website that contains Improper Material (Exception: sanctioned law enforcement employees performing assigned investigative work). The County reserves the right to block employee access to such web sites.

4. No employee shall operate or advertise any non-County business on the Internet using County equipment at any time.

5. No employee shall send chain letters, pyramid schemes, or unsolicited bulk email using County equipment at any time.

6. No employee shall use official County email addresses to distribute jokes, virus warnings, sentimental missives, rumors, political commentary, or other non-work-related material to other employees or the general public. (NOTE: Only IT employees are to transmit virus warnings.)

7. Personal usage of County email, Internet or electronic devices should not impede the conduct of County business; only occasional and incidental amounts of employee time comparable to reasonable coffee breaks during the day should be used to attend to personal matters. Questions regarding the extent of this policy should be discussed with Department Heads/Elected Official. Personal use of

Internet resources is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.

8. All employees shall use only their County-assigned email address during the performance of their assigned job duties. No private or "ghost" accounts shall be used, except by network administrators as part of their function (e.g., account names like "Webmaster," "Postmaster," "root," etc.) and special investigations. All requests for exceptions to this policy must be approved by the IT Director.

9. Email received from citizens should be handled with the same seriousness and professionalism as any other form of citizen contact. Employees should always maintain professional decorum in their responses, seek approval from supervisors where appropriate, and reply to messages promptly.

10. Unless specifically approved by the IT Director, all Internet email transmissions shall be routed though the official County gateway service (Exception: sanctioned law enforcement employees performing assigned investigation work). No department or employees shall operate within County networks any email servers, mail forwarding services, or other email transmission or reception services for use by any person or automated system.

11. Internet traffic will be filtered to prevent access to inappropriate sites and those deemed detrimental to network services.

F. Personal Device Usage

1. The County of Victoria reserves the right to disconnect, or prevent connection to County network resources of any device, by any user, at any time, or for any reason, without any notice whatsoever.

2. Employees must contact the IT Help Desk to determine whether their device is eligible, and to obtain proper user credentials for their device. The IT Director, or designee, shall be solely responsible for determining which devices may be connected to County resources.

3. The employee attaching their personal device to a County network resource assumes full liability for any risks, including, but not limited to, partial or complete data loss, errors, bugs, hardware loss or damage, viruses, malware, or any other issue which may damage the device, in any way whatsoever. The employee assumes all risk by connecting to the resource.

4. Support - The IT department will provide support for network connectivity issues. However, hardware and software support for personal devices will not be provided.

5. Reimbursement - Connection to County-owned network resources is provided to employees as a convenience only. The County will not reimburse any expense, partial or otherwise, for any usage of a personal device, including cell phones, regardless of purpose.

6. Personal Device Security

    a) No personal devices shall be connected to the County network without approval from the IT Department.
    b) Personal devices and visitor devices are allowed to connect to the "GUEST" WIFI.

G. Communications Network

1. No employee or other person shall install or move any network device onto the County communications network under any circumstances whatsoever. Only members of the IT department are permitted access to such equipment.

2. No employee, contractor, or third party may install any device or software intended to monitor, capture, or eavesdrop upon, any portion of data traversing the County Network, excepting members of IT.

3. Employees shall not attach any form of personal network equipment including, but not limited to, switches, routers, or modems to any County network.

4. No employee will permit any third party to connect any device to any Ethernet jack or secure wireless service without the express permission of the IT Director or designee, unless service is specifically provided for such purpose.

5. No employee shall install or operate any equipment or service which has the effect of redirecting or proxying any network traffic to or from any other network, or disguising the source of any network transmission.

H. Software

1. The County is committed to preventing copyright infringement. It is the policy of the County of Victoria to respect all computer software copyrights and to adhere to the terms of all software licenses to which the County is a party. The County is subject to all copyright laws pertaining to the use of copyrighted software and documentation. Unless expressly authorized by the software licensor/developer, the County of Victoria has no right to make copies of the software except for backup or archival purposes.

2. All software used on a County computer must be licensed to the County for that computer.

3. Employees may not install any software not provided to them by the IT Department without specific authorization by the IT Director or designee.

4. County employees shall not duplicate, copy, or reproduce any software purchased by and/or licensed to the County, or any related documentation without prior written approval from the IT Director. County employees shall not give County-purchased or licensed software to any non-employees, including, but not limited to clients, contractors, customers, and others without prior written approval from the IT Director.

5. Software developed by employees on County time, or on County-owned equipment, or for County projects, shall be the property of the County. Such software is for the exclusive use of the County, its officers, agents, and employees. Such software may not be sold, transferred, or given to any person without the prior written approval of the County Judge or designee.

6. Software must be registered in the name of the County and the Department in which it will be used. Software shall not be registered in an individual employee user's name.

7. Game software is an inappropriate use of County equipment and shall not be tolerated on desktop PCs. Games discovered during audits shall be eliminated and the employee user may be subject to disciplinary action.

I. Personal and County Issued Mobile Devices, Cellular Telephones and Cell Phone Allowances:

1. Eligibility Criteria – Employees eligible for assignment of County owned mobile devices or Cell Phone Allowances will be requested by the Department Head/Elected Official and approved by the IT Director & Human Resources (Exception: sanctioned law enforcement employees who are assigned phones) if it is within the office/departments budget. If any budget amendment or request for additional funds is needed the request must also go through Commissioners' Court for approval.

a) The procedures set forth in Section III. of this document for County computers and telecommunications resources shall also apply to County owned and issued mobile devices and cellular phones.

a) Users must understand that using their personal device to conduct County business (regardless of whether or not a cell phone allowance is in place) may impose the possibility of open records access responsibility. This means you may be required to provide records from your personal device or submit your personal device to a search for either an open records or legal request if it accesses County systems.

b) Improper use of the County's owned devices may result in disciplinary action, up to and including termination.

J. Security - It is the responsibility of every employee to operate all County telecommunications, computer, or other electronic equipment in such a way as to minimize the risk of unauthorized access to, or loss of, any County resource by any other party, to ensure that County resources are not misused by any other person, and to act so as to protect the integrity of the data and resources of the County.

1. Password Policy - Each County employee (who uses computers) must have a unique password.

a) Passwords may not be written down where they can be found by unauthorized personnel or be shared with other individuals. It is the responsibility of the employee to maintain the secrecy of their passwords. Employees cannot provide their passwords to anyone, including family members.

b) Passwords are to be reset regularly to maintain security.

c) If an employee is concerned their password has been compromised they are to notify the IT Director and change their password.

2. All employees shall immediately report any unauthorized access or unauthorized access attempt, virus infection, spyware infection, or other unauthorized or illegal resource use to the IT Director or his designee.

3. Employees shall not download or install any software of any kind whatever from the Internet or any storage device or media to any County-owned computer without the prior consent of the IT Director.

4. Employees shall not insert or connect any phones or devices to County computers or networks (even for charging purposes) without prior approval from the IT Director.

5. Employees shall not insert or connect any USB devices, CDs, or storage devices to any County computer or network without knowledge of the storage device’s origins and contents. If a USB, CD or other storage device is found by or sent to an employee and the employee has no knowledge of what is on the device it must be reviewed and approved by the IT Director for use.

6. Lost, stolen or seized property must be reported to IT Director and Human Resources with 24 hours.

K. Technology Procurement

1. Departments will coordinate all technology or software related purchase requests (including grant proposals, RFPs, bids, contracts, purchase orders, and County credit card purchases) with the IT Director or designee verbally or in writing prior to purchase. The purpose of this review is:

   a) To ensure that the product(s) obtained are compatible with County standards and existing infrastructure;

   b) To avoid unnecessary and costly duplication of capabilities;

   c) To minimize impacts on support personnel;

   d) To ensure all costs are properly considered; and

   e) To ensure that the proposed equipment or software does not interfere with the operation of existing systems, or create any undue risk to County resources.

   f) Departments will involve the IT department in the earliest planning stages of any grant proposal, RFP, bid, contracts, or purchase, etc., which will result in IT related services or products being obtained, prior to the submission of any request to the Commissioners' Court.

L. IT and Cyber Security Training - It is the responsibility of every Department Head/ Elected Official to identify any and all employees who may have access to Victoria County computers or networks within their Office/Department. Every Victoria County Office/Department will work in conjunction with the IT Department and Administrative Services to ensure that all employees with access to County networks and computers receive yearly training required by law to protect Victoria County's Information Technology and Cyber Infrastructure.

1. It is the responsibility of the Department Head/Elected Official to notify the IT Department at least three working days prior to the start date of any new employee or authorized user who will be required to have training required by law to protect Victoria County's Information Technology and Cyber Infrastructure.