Recommended Technology Policy

Proposed Action for County Road Commissions

July 1, 2017

Liability | Strategic Risk Management Guideline | Issue SRM201707-7

How Road Commissions can address the ever increasing security threats they face on the internet

A technology policy provides standards and safeguards to protect an organization's IT assets and sensitive data. It is important as well for employees to understand what is expected of them with the technology that your road commission provides them.

This guideline contains a recommended Technology Policy for your road commission to adopt. It covers the following areas:

1 & 2. Technology Hardware and Software Purchasing – Ensures that all hardware/software is appropriate, and integrates with the existing technology at your road commission.

3. Use of Software – Covers software licensing, installation, and its use at your road commission.

4. Bring Your Own Device (BYOD) – Important guidelines to implement for employees who want to use their own mobile devices to connect to your road commission's network and equipment.

5. IT Security – Helps ensure the integrity, confidentiality, and availability of data and assets.

6. Password Policy – Designed to make sure users are changing their passwords regularly to minimize the threats by hackers and non-authorized employees seeking to gain access to your system and data.

7. Remote Access – Guidelines to help minimize the potential exposure which can result when employees work remotely.

8. Internet Usage – Ensures your employees are using the internet responsibly and productively.

9. Hardware Destruction – Ensures that the information on your devices is adequately removed or destroyed before being sold or transferred to another department.

10. Security Procedures for Terminated Employees – This will minimize the security risk to your road commission by former employees.

The Serious and Growing Danger of Cyber Attacks

•••

"Cyber crime…is the greatest threat to every profession, every industry, every company in the world."
– Ginni Rometty, IBM Chairman, President and CEO

"One single vulnerability is all an attacker needs."
– Window Snyder, Chief Security Officer, Fastly

"More than 4,000 ransomware attacks have occurred every day since the beginning of 2016. That's a 300% increase over 2015, where 1,000 ransomware attacks were seen per day."
– Computer Crime and Intellectual Property Section (CCIPS)

Technology Policy

1. Technology Hardware Purchasing

Purpose

This section provides guidelines for the purchase of hardware for the **{name of road commission)** to ensure that all hardware technology is appropriate, a value for the money and, where applicable, integrates with other technology for the business. The objective is to ensure that there is minimum diversity of hardware within the business.

Procedures

Purchase of Hardware

All hardware purchases must be approved by the **{title}**

{Contact information of vendor}:

Purchasing desktop computer systems

The desktop computer systems purchased must run at least **{operating system}** and integrate with existing hardware.

The desktop computer systems must be purchased as standard desktop system bundle and must be **{approved brands, e.g., HP, Dell}**.

The desktop computer system bundle must include:

Desktop tower

Desktop screen of **at least {size of screen}**

Keyboard and mouse, wireless or non-wireless.

- **{operating system}**
- **{additional spec}**

The minimum capacity of the desktop must be:

- **{processor}**
- **{memory}**
- **{hard drive}**

- **{# USB ports}**

Any change from the above requirements must be authorized by the **{title}**.

All purchases of desktops must be compatible with the road commission's server system.

Purchasing portable computer systems

The purchase of portable computer systems includes notebooks, laptops, and tablets.

Portable computer systems purchased must run **{operating system}** and integrate with existing hardware. The portable computer systems purchased must be **{approved brands, e.g., HP, Dell}**.

The minimum capacity of the portable computer system must be:

- **{processor}**
- **{memory}**
- **{hard drive}**
- **{# USB ports}**

The portable computer system must include the following software provided:

{list of programs}

Any change from the above requirements must be authorized by the **{title}.**

Purchasing server systems

Server systems can only be purchased by the **{title}.**

Server systems purchased must be compatible with all other computer hardware in the road commission.

All purchases of server systems must be compatible with the road commission's other server systems.

Any change from the above requirements must be authorized by the **{title}.**

Purchasing computer peripherals

Computer system peripherals include printers, scanners, external hard drives, etc.

Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.

Computer peripherals purchased must be compatible with all other computer hardware and software in the business.

The purchase of computer peripherals can only be authorized by the **{title}**.

Any change from the above requirements must be authorized by the **{title}**.

Purchasing mobile telephones

A mobile phone will only be purchased once the eligibility criteria is met. Refer to the Mobile Phone Usage policy in this document.

The purchase of a mobile phone must be from **{vendor name}** to ensure the business takes advantage of volume pricing based discounts provided by **{vendor or program name}**. Such discounts should include the purchase of the phone, the phone call and internet charges, etc.

{vendor contact information}:

The mobile phone must be compatible with the road commission's current hardware and software systems.

The mobile phone purchased must be **{product names}**.

The purchase of a mobile phone must be approved by the **{title}** prior to purchase.

Any change from the above requirements must be authorized by the **{title}**.

2. Software Purchasing

Purpose

This section provides guidelines for the purchase of software for the **{name of road commission}** to ensure that all software used is appropriate, a value for the money and, where applicable, integrates with other technology for the business. This section applies to software obtained as part of hardware bundle or pre-loaded software.

Procedures

Request for Software

All software, including any non-commercial software such as open source, freeware, etc. must be approved by the **{title}** prior to the use or download of such software.

Purchase of software

The purchase of all software must adhere to this policy.

All purchased software must be purchased by the **{title}**.

All purchased software must be purchased from reputable software sellers, such as **{name of sellers}**.

All purchases of software must be compatible with the road commission's server and/or hardware system.

Any changes from the above requirements must be authorized by the **{title}**.

Obtaining open source or freeware software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

In the event that open source or freeware software is required, approval from the **{title}** must be obtained prior to the download or use of such software.

All open source or freeware must be compatible with the road commission's hardware and software systems.

Any change from the above requirements must be authorized by the **{title}**.

3. Use of Software

Purpose

This section provides guidelines for the use of software for all employees within the **{name of county road commission}** to ensure that all software use is appropriate. The use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

Procedures

Software Licensing

All computer software copyrights and terms of all software licenses will be followed by all employees of the business.

Where licensing states limited usage (i.e., number of computers or users, etc.), then it is the responsibility of the **{title}** to ensure these terms are followed.

The **{title}** is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and license agreements are adhered to.

Software Installation

All software must be appropriately registered with the supplier where this is a requirement.

{Name of road commission} is to be the registered owner of all software.

Only software obtained in accordance with the purchasing software section of the policy is to be installed on the road commission's computers.

All software installation is to be carried out by the **{title}**.

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

Software Usage

Only software purchased in accordance with the purchasing software section of the policy is to be used within the business.

Prior to the use of any software, the employee must receive instructions on any licensing agreements related to the software, including any restrictions on use of the software.

All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of the **{title}**

Employees are prohibited from bringing software from home and loading it onto the road commission's computer hardware.

Unless express approval from the **{title}** is obtained, software cannot be taken home and loaded on an employee's home computer.

Use of Software (continued)

Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorization from the **{title}** is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of **{name of county road commission}** and must be recorded on the software register by the **{title}**.

Unauthorized software is prohibited from being used at **{name of county road commission}**. This includes the use of software owned by an employee and used within the organization.

The unauthorized duplicating, acquiring, or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorized copies of software will be referred to the **{title}** for further review, discussion and/or reprimand. The illegal duplication of software or other copyrighted works is not condoned within this organization and the **{title}** is authorized to undertake disciplinary action where such event occurs.

Breach of this Policy

Where there is a breach of this section of the policy by an employee, that employee will be referred to the **{title}** for further review, discussion and/or reprimand.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the **{title}** immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then that employee will be referred to the **{title}** for further review, discussion and/or reprimand.

4. Bring Your Own Device (BYOD)

At **{name of road commission}** we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to the road commission's network and equipment.

Purpose

This section of the policy provides guidelines for the use of personally owned notebooks, smart phones, and tablets for business purposes. All staff who use or access **{name of road commission}**'s technology equipment and/or services are bound by the conditions of this policy.

Procedures

Current mobile devices approved for business use

The following personally owned mobile devices are approved to be used for business purposes:

- **{approved device}**
- **{approved device}**
- **{approved device}**

Registration of personal mobile devices for business use

When using personal devices for business use, employees will register the device with the **{title}**, who will record the device and all applications used by the device.

Personal mobile devices can only be used for the following business purposes:

- **{list purposes, e.g., email access, business internet access, business telephone calls}**.

Each employee who utilizes personal mobile devices agrees:

- Not to download or transfer business or personal or sensitive information on **{categories of information e.g., employee, county residents, etc.}.**
- Not to use the registered mobile device as the sole repository for **{name of road commission}**'s information. All business information stored on mobile devices should be backed up.
- To make every reasonable effort to ensure that **{name of road commission}**'s information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorized persons and all registered devices should be password protected.

BYOD (continued)

- To maintain the device with security software provided by **{name of road commission}**'s outside technology services provider.
- Not to share the device with other individuals to protect the business data access through the device
- To abide by **{name of road commission}**'s internet policy for appropriate use and access of internet sites etc.
- To notify **{name of road commission}** immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to **{name of road commission}**'s equipment.

All employees who have a registered personal mobile device for business use acknowledge that **{name of road commission}**

- Owns all intellectual property created on the device.
- Can access all data held on the device, including personal data
- Will regularly back up data held on the device
- Will delete all data held on the device in the event of loss or theft of the device
- Has first right to buy the device when the employee wants to sell the device
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
- Has the right to deregister the device for business use at any time.

Keeping mobile devices secure

The following must be observed when handling mobile computing devices such as notebooks and iPads:

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away.
- Cable locking devices should also be considered for use with laptop computers in public places (e.g., in a seminar or conference) even when the laptop is attended.
- Mobile devices should be carried as hand luggage when traveling by aircraft.

Exemptions

This policy is mandatory unless the **{title}** grants an exemption. Any requests for exemptions from any of these directives, should be referred to the **{title}.**

Breach of this policy

Any breach of this section of the policy will be referred to the **{title}** who will review the breach and determine adequate consequences, which can include confiscation of the device and or termination of employment.

Indemnity

{Name of road commission} bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify **{name of road commission}** against any and all damages, costs and expenses suffered by **{name of road commission}** arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by **{name of road commission}**.

5. IT Security

Purpose

This section provides guidelines for the protection and use of information technology assets and resources within the **{name of road commission}** to ensure integrity, confidentiality, and availability of data and assets.

Procedures

Physical Security

For all servers, mainframes, and other network assets, the area must be secured with adequate ventilation and appropriate access through **{description of security}**.

It will be the responsibility of **{title}** to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify **{title}** immediately.

All security and safety of all portable technology, laptops, iPhones, iPads, etc. will be the responsibility of the employee who has been issued with the device(s). Each employee is required to use password protection on all devices and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, **{title}** will assess the security measures undertaken to determine if the employee will be required to reimburse the **{name of road commission}** for the loss or damage.

All issued electronic devices when kept at the office desk are to be secured by password protection provided.

Technology Access

Every employee will be issued with a unique identification code to access the business technology.

Where an employee forgets the password or is ‘locked out’ after three attempts, then the **{title}** is authorized to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

It is the responsibility of the **{title}** to keep all procedures for this policy up to date.

6. Passwords

Purpose

This section is designed to make sure users are changing passwords on a regular basis and to verify the passwords are strong enough to handle brute force attacks to minimize the impact of hacker, employee, etc. from gaining unauthorized access to the system.

Procedures

Password requirements

The road commission's employees are expected to use complex passwords. Complex passwords are defined by being 10 characters in length, containing one number, and one symbol such as $%@#.

Passwords will change every 90 days in an effort to prevent people from having someone else's password.

Remote access passwords are to be used only by the individuals to whom they were assigned and may not be shared.

All passwords, unless with written permission, will not be shared.

All vendors will have separate usernames and passwords that also change every 90 days.

All devices, including firewalls, routers, switches, DVRs, cameras, and printers will change default passwords.

Firewall passwords will change every 180 days.

Local login passwords will need to be changed from default of system.

At no time is an eight character password, blank password, or default password ever permitted.

All company cell phones will be password restricted.

Applies

Password policies are enforced to the following areas: wireless network (guest and production), local computers, Active Directory, firewalls, routers, switches, printers, organization phones, email, and **{name of road commission}'s** website.

Breach of this policy

Any employee found to have violated this section of the policy may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.

7. Remote Access

Purpose

These requirements are designed to minimize the potential exposure from damages which may result from unauthorized use of **{name of county road commission}** resources. Damages include the loss of sensitive and/or confidential information, damage to public image and damage to critical internal systems.

Procedures

General

Storage of confidential information on any non-organization owned device is prohibited. Confidential information may not be stored on any non-organization owned portable device without prior written approval from the supervisor (or delegated authority). Approved storage on any portable device must be encrypted.

It is the responsibility of the road commission employees and contractors with remote access privileges to the organization's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the company.

All remote access users are expected to comply with the road commission's policies, may not perform illegal activities, and may not use the access for outside business interests.

Requirements

Remote access must be strictly controlled by the use of unique user credentials. For more information, please view Password Policy.

Remote access passwords are to be used only by the individuals to whom they were assigned and may not be shared.

All remote access connections that utilize a shared infrastructure, such as the internet, must utilize some form of encryption.

Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

All hosts that are connected to the road commission's internal networks via remote access technologies must have up-to-date anti-virus software implemented.

All hosts that are connected to the road commission's internal networks via remote access technologies must have current operating system security patches installed.

Personal equipment that is used to connect to the company's networks must meet the requirements of the road commission-owned equipment for remote access.

Organizations or individuals who wish to implement non-standard remote access solutions to the road commission production network must obtain prior written approval from **{name of road commission}**.

Breach of this policy

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.

Definitions

Term	Definition
Cable Modem	Cable companies provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP).
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems.
Remote Access	Any access to the corporate network through a non-company controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-company network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into the corporate network via a VPN tunnel. Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.
Wi-Fi	Wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A Wi-Fi enabled device such as a PC, mobile phone, or PDA can connect to the Internet when within range of a wireless network.

8. Internet Usage

Purpose of the Policy

These requirements are designed to minimize the potential exposure from damages which may result from unauthorized use of **{name of county road commission}** resources. Damages include the loss of sensitive and/or confidential information, damage to public image, and damage to critical internal systems.

Procedures

Computer, Email and Internet Usage

{name of county road commission} employees are expected to use the internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted.

Job-related activities include research and educational tasks that may be found via the internet that would help in an employee's role.

All internet data that is composed, transmitted and/or received by a road commission's computer systems is considered to belong to the road commission and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

The equipment, services and technology used to access the internet are the property of **{name of county road commission},** which reserves the right to monitor internet traffic and monitor and access data that is composed, sent or received through its online connections.

Emails sent via the company email should not contain content that is deemed to be offensive.

All sites and downloads may be monitored or blocked by **{name of road commission}** if they are deemed to be harmful and/or if the road commission deems it not productive to business.

The installation of software such as instant messaging technology is strictly prohibited unless otherwise stated by **{name of road commission}**.

Unacceptable use of the internet by road commission employees includes, but is not limited to:

Sending or posting discriminatory, harassing, or threatening messages or images on the internet or via the road commission's email service.

Using computers to perpetrate any form of fraud, and/or software, film or music piracy.

Stealing, using, or disclosing someone else's password without authorization.

Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.

Internet Usage (continued)

Sharing confidential material, trade secrets, or proprietary information outside of the organization.

Hacking into unauthorized websites.

Sending or posting information that is defamatory to the organization, its products/services, colleagues and/or customers.

Introducing malicious software into the road commission's network and/or jeopardizing the security of the organization's electronic communications systems.

Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.

Passing off personal views as representing those of the organization.

9. Hardware Destruction

Purpose

These requirements outline the proper disposal/sanitization/destruction of media (physical or electronic) at **{name of road commission}**. These rules are in place to protect sensitive and classified information, employees and **{name of road commission}**. Inappropriate disposal of **{name of road commission}** may put employees at **{name of road commission}** at risk.

Procedures

Standard

Licensed Software programs, institutional/business data, personally identified or identifiable data, and/or non-public data must be reliably erased and/or destroyed from any electronic device before the device is transferred out of **{name of road commission}** control or erased before being transferred from one **{name of road commission}** department or individual to another. Failure to properly purge data correctly that renders the data unrecoverable may pose a risk to **{name of road commission}**'s data since data often can be easily recovered with readily available tools.

Disposal

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, printouts, and other similar items used to process, store and/or transmit classified and sensitive data shall be properly disposed of in accordance with measures established by **{name of road commission}**.

Physical media (printouts and other physical media) shall be disposed of by one of the following methods:

- Shredded using **{name of road commission}** issued cross-cut shredders
- Placed in locked shredding bins for **{name of vendor}** to come on-site and cross-cut shred, witnessed by **{name of road commission}** personnel throughout the entire process
- Incineration using **{name of road commission}** incinerators or witnessed by **{name of road commission}** personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel.

Electronic media (Hard drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one of the **{name of road commission}**'s methods:

- Overwriting (at least 3 times) – An effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) into the location of the media where the file is to be sanitized is located.
- Degaussing – A method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that

common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

- Destruction – A method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically destroy by methods of crushing, disassembling, etc. ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store or transmit sensitive and classified information shall not be released from **{name of road commission}**'s control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Process

No computers or digital storage devices may leave **{name of road commission}**'s possession without undergoing the described sanitization methodology.

Documentation, for potential audit purposes, attesting to the erasure of licensed software and institutional data is required in order to complete the transfer both within and external to **{name of road commission}**, including devices for trade-in or that must be replaced as part of a warranty or repair contract. Documentation should be retained securely at each **{name of road commission}**'s site.

Penalties

Any **{name of road commission}** employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

10. Security Procedures for Terminated Employees

Purpose

These requirements are designed to minimize the security risk to **{name of county road commission}'s** network by terminated employees.

Procedure:

When an individual's employment with **{name of road commission}** is terminated, for any reason, the **{title}** will adhere to the following procedures:

Regular Users Process — Upon notification of the termination by the **{title}**, immediately disable the terminated employee's:

- Email Account
- Network Account
- Voice Mail System
- VPN/Remote Access Accounts
- Web-meeting & Collaboration accounts
- All application accounts
- Access to any road commission financial accounts
- Access to road commission information/data backups
- Access to road commission owned social media accounts or web properties

IT Privileged Users Process — For users with system administration privileges the account termination process must be even more extensive. A thorough analysis to determine the extent of the person's access should be conducted to validate that all access is terminated as expected. Special attention should be paid to:

- Database accounts
- Application level service accounts
- Accounts with shared passwords
- Network/Router passwords
- Generic test accounts
- Remote access accounts including VPNs, Jump boxes or even analog modem connections