Le Sueur County, MN

Tuesday, February 17, 2015

Board Meeting

Item 5

10:25 a.m. BYOD Policy (15 min)

Staff Contact: Scott Gerr--MIS

Le Sueur County Wireless Telecommunication Device User Agreement

Purpose

Le Sueur County supports the use of Wireless Telecommunication Devices, including cell phones, smart phones, tablets as an efficient tool for accomplishing work. Because an efficient administrative process is desired, County-wide policy and procedures regarding the purchase and use of Wireless Telecommunication Devices has been developed.

Policy and Appropriate Use

It is the responsibility of any employee of Le Sueur County who uses a wireless device to access County data/resources to ensure that all efforts be made to protect the security of the data, including adherence to the Le Sueur County Wireless Telecommunication Device Policy and abiding by security requirements identified for wireless equipment.

Access Control

Le Sueur County reserves the right to authorize access to the County network or County–connected infrastructure whether through County-owned wireless devices or personally owned equipment. An employee considering the use of personally owned equipment is required to consult with IT to confirm that the device is capable of supporting a County connection.

The County reserves the right to refuse, by physical and non-physical means, the ability to connect a wireless device to County and County-connected infrastructure. Devices that do not meet requirements may not be connected to the County infrastructure. The County reserves the right to remain current with security requirements and/or changes in technology. The county reserves the right to remotely wipe a mobile device that has been lost or stolen. In general all devices must:

- Utilize screen lock\password capability
- Support the Microsoft ActiveSync (Exchange ActiveSync) application allowing a mobile device to synchronize with either a desktop PC or Le Sueur County's email server.
- Add any additional mobile device management software as adopted by the Information Technology Department for secure login and data security enforcement.

Security

All mobile devices connected to the County infrastructure must conform to minimum security standards published by Le Sueur County. In the event that a mobile device connected to the County network is lost or stolen, it is the responsibility of the user of that device to immediately report the loss to their supervisor or the IT Department. The employee is also responsible for notifying their service provider.

Employees using mobile devices and related software for network and data access will use the security features prescribed by the County including password protection and encryption. Any mobile device that is being used to store Le Sueur County data must adhere to the authentication requirements of Le Sueur County.

The Le Sueur County Information Technology Department will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with County Personnel Policies.

All employees must allow the Information Technology Department to remove County specific data and software from their personal wireless device when such data are no longer required.

Wireless Authorization

This signed agreement must be completed prior to connecting personal devices to County-owned resources.

Help & Support

The level of support provided for personally owned and approved wireless devices is limited to supplying necessary information for connecting to the Le Sueur County network. Information Technology is not responsible for the training, use or technical

I, _____ have read and agree to the Le Sueur County Wireless Telecommunication Device Policy and User Agreement. I understand and agree to remove all County-specific data from my personal wireless device when such data is no longer required; and I will immediately report lost or stolen wireless devices to the Le Sueur County IT Department and my supervisor.

Employee Signature: _____ Date: _____

Supervisor Review

Request is Approved ☐ Denied ☐

Supervisor Signature: _____ Date: _____

Department Head Review

Request is Approved ☐ Denied ☐

Department Head Signature: _____ Date: _____

Information Technology Director Review

Request is Approved ☐ Denied ☐

IT Director Signature: _____ Date: _____

County issued phone number: ☐ IT Master list updated

Le Sueur COUNTY
Wireless Telecommunication Device Policy

POLICY STATEMENT

The purpose of this policy is to define standards, procedures, and expectations for any users who access County data from mobile devices connected to external networks outside of Le Sueur County's direct control.

This policy recognizes that now and in the future, Le Sueur County business will be conducted on both County-owned and personally-owned mobile devices. This policy must be followed by all mobile device users no matter who owns the device.

Examples of mobile devices that this policy applies to include: cellular smartphones, tablets, e-readers, and other similar mobile wireless devices with computing functionality. This list is not exhaustive, will change over time, and is intended for illustration only.

The primary goal of this policy is to protect the integrity of the private and confidential client and business data that resides within Le Sueur County's technology resources, particularly when it is accessed by or transferred to mobile devices which, by their very nature, can be easily lost or stolen. This policy is intended to prevent these data from being deliberately or inadvertently stored insecurely on a mobile device, or carried over or stored on an insecure network, where the data potentially can be accessed by unsanctioned resources or persons. A breach of this type could result in loss of information, damage to critical applications, damage to the County's public image and liability to the County or third persons. Therefore, all users employing a mobile device connected to an external network outside of Le Sueur County's direct control to backup, store, and otherwise access County data or technology resources must adhere to County-defined policies and processes for doing so.

Secondary goals of this policy are to help employees work with maximum efficiency and to ensure accountability of public funds entrusted to Le Sueur County.

DEFINITIONS

Business use: work-related responsibilities required by an employee's position or role assigned by the employee's supervisor, manager, department head or other county official.

Convenience-level access: using the operating system of the device when purchased from the manufacturer users can connect (i.e. synchronize their device) to Le Sueur County's email network through its mobile device management system. This level of access limits users to see email, calendar, contacts and tasks data that make up the County's email system.

County email system: Data and services associated with the County-provided email system including calendaring, contact information, task management, etc. (also known as "Outlook" by users).

County-owned: a device that is purchased by, and provisioned by, Le Sueur County for use by County employees or associates[1]. ***County-sanctioned devices*** are devices that are not owned by the County, but may instead be used by employees or associates of the County for county business use.

Data Security Officer: An employee in the Information Technology department who is responsible for developing and implementing a security risk management program for the County's technology resources; publishing enterprise-wide security policies, procedures, and responsibilities; and providing programs and processes to implement these security risk management policies.

[1] Associates are defined as people who are not employees but who work within County facilities or its networks to provide services to the County. Associates may include employees of vendors or contractors, interns, volunteers, or others.

Designee: For purposes of this policy, designee means one or more individuals to whom the County Administrator has delegated authority under this Policy by written delegations, which identify the authorities delegated, the individuals to whom authority is delegated, and the duration of the delegation. This written delegation document will be maintained on file with the Clerk to the Board.

Information Technology department (IT): IT staff provide services to all County employees who require telephone or computing technology hardware and software to perform their jobs. IT services include project management and business analysis, software development, maintenance, support, security and administration for: web-based applications, third-party applications, client records and document management systems, databases, the County's intranet and external website, and all virtual and physical desktop or mobile devices.

Mobile device: A tablet computer, mobile phone (also known as a "smart" phone), or other portable device with a proprietary operating system that is small enough to be easily transported and conveniently used in temporary remote work locations such as client settings, airplanes, libraries, temporary offices, and off-site meetings.

Mobile device management (MDM): a software system that acts as an over-the-air electronic gateway between an array of mobile devices and an organization's data and networks. MDM also blocks unauthorized users from synchronizing with technology resources and enforces device registration, authenticates users, encrypts data in transit and at rest on the device, enforces security protocols such robust passwords, and can remotely wipe (delete) all business-related data from devices that are compromised. Also known as a Mobile Applications Management system.

Mobile phones: Also known as "cellular phones", "cell phones", or "smart phones", a portable electronic device used for mobile voice or data communication over a network of specialized base stations.

Personally-owned or privately-owned devices: For the purposes of this policy, computing devices such as mobile phones and tablet computers that have been purchased and are maintained exclusively by an employee, county elected official, contractor, intern, or volunteer, and that are used for mobile voice or data communication for both business and personal use.

Provisioned: software or other customized operations system changes, including those necessary to support security protocols, installed on mobile devices by either the County or a device manufacturer. Applications for tablets may also be County-provisioned so that devices connect with County technology resources.

Technology resources: all of the components required to deliver or access IT services, including hardware, software, telecommunications, data networks, infrastructure, and other similar components.

Users: any elected official, employee (i.e., a person who is appointed to a non-limited or limited term of employment, contractor, vendor, intern, or volunteer who is provided access to Le Sueur County data or networks for business purposes.

GENERAL

SCOPE and APPLICABILITY

This policy relates to the purchase, use of, and connectivity to County technology resources, whether by personally-owned or County-issued devices. It applies to all Le Sueur County elected officials, employees (including full and part-time staff), temporary staff, interns, volunteers, and contractors or vendors who use either a County-owned or personally-owned mobile device to access County technology resources such as any County data on any County network. Access to technology resources is a privilege, not a right, and employment at Le Sueur County does not automatically guarantee the initial and ongoing privilege to use mobile devices to gain access to County technology resources.

Employees will follow all local, state, and federal regulations regarding the use of mobile devices while operating motor vehicles or heavy machinery. If possible, employees should pull off the road or use a hands-free devise to conduct legally-allowed business using a mobile device while operating a motor vehicle. The Sheriff's Office may promulgate supplemental policies which will supersede the application of this section to licensed law enforcement employees.

All work-related photographs and/or videos captured on a County-owned mobile device are considered governmental data and shall be transferred to government computers for proper documentation and storage promptly. Similarly, all work-related photographs and/or videos captured on a non-County-owned mobile device are also considered governmental data and shall be transferred to government computers for proper documentation and storage promptly. Employees must exercise discretion with personal use of mobile devices when using a County-owned mobile device.

Employees authorized to use text messaging for County business may only do so for messages that do not need to be retained by Le Sueur County. Examples include notices of meetings, directions, and non-protected scheduling information, and other routine messages that would not be filed if it were a paper communication. Employees are prohibited from using text messages to send policy, contract, personnel or private client-related County data. Employees are prohibited from sending text messages containing governmental information classified as confidential, private, or non-public in Chapter 13 of Minnesota State Statute. If text messages need to be saved under Le Sueur County retention policies, employees must be able to transfer messages to their Department's network drive.

If a question arises regarding the retention of an electronic communication on a mobile device, the employee shall analyze the information and determine whether retention is required by federal, state or local regulations or policies. All users, of either County-owned or non-County-owned mobile devices, shall preserve all governmental data required to be maintained pursuant to the adopted records retention schedule of Le Sueur County for the required period on a County-owned server in a format that preserves the integrity of the original record and is easily accessible as required by state and federal laws.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the County network.

CRITERIA

Device ownership preference

Based on necessity for his/her job, Le Sueur County's first preference is for employees to use personally-owned devices for approved business uses. The second preference is for Le Sueur County to approve County-owned mobile devices for employees to use as necessary to perform their work functions.

Nonexempt employees who access County systems with mobile devices may not work non-shift hours without authorization or direction from a supervisor.

Compliance and Data Maintenance

All employees who access County technology resources using a mobile device must sign a user agreement, which is time-limited and must be reviewed and renewed annually. As part of this process, employees are responsible for updating their list of active devices with the County.

IT staff provide department heads annually with a list of employees who access county data/networks using mobile devices under this policy. Department heads must review this list and confirm with IT staff that access has been terminated for:

- current employees who no longer require access,
- devices that are no longer in use,
- users who are on unpaid leave or whose access has otherwise been eliminated by department managers,
- or users who are no longer employed by Le Sueur County, so that their access can be terminated.

AFFECTED TECHNOLOGY

Any device remotely connecting to the County's technology resources must be manufactured with software that allows connectivity and synchronization. Such devices must also be compatible with the County's Mobile Device

Management (MDM) system. Not all personally-owned devices come with software that allows this connectivity. Connectivity of all mobile devices will be centrally managed by the Le Sueur County IT department and will require use of security protocols such as authentication and strong encryption measures, as outlined in the user agreement.

PROCEDURES

If the MDM system fails for any reason, or some other network-wide technology system fails, all mobile device users with access to County technology resources must ensure that all security protocols normally used in the management of County data continue to be followed. It is imperative that any mobile device that is used to conduct Le Sueur County business be used appropriately, responsibly, and ethically. Failure to do so may result in immediate suspension of the user's access privileges to County technology resources in order to protect the County's data and technology resources.

ACCESS CONTROL

1. Le Sueur County, through its Information Technology Director, reserves the right to refuse to connect or to remove the connection of mobile devices to the County's technology resources if the County reasonably believes that the mobile devices pose or might pose a risk to the County's technology resources, data, users or clients, or if otherwise deemed appropriate by management.

2. Any personally-owned devices must have sufficient minimum functionality to allow security protocols (such as encryption, password lockouts, and others) in order for them to be connected to County technology resources. Such devices must also be compatible with the County's MDM system.

SECURITY

3. For any devices connected to County technology resources that are lost or stolen, whether County owned or personally owned, the user of that device shall immediately report the loss to the Le Sueur County Help Desk and the user's supervisor.

   When notified by Help Desk staff, the Data Security Officer will follow the established guidelines to determine next steps. If the device is owned by the user, the user is responsible for notifying his/her wireless service provider of the loss or theft.

4. Le Sueur County, through its Information technology Director, intends to remotely delete or wipe business- related messages and data from mobile devices, including personally-owned mobile devices, when the device has been reported to be lost or stolen. While Le Sueur County intends that the capability of its mobile device management system will not be used to delete personal messages and data from personally-owned devices, Le Sueur County cannot and does not guarantee that such personal messages and data will never be remotely deleted or wiped. Prudent owners of mobile devices should back up their personal messages and data that are stored on their personal devices.

5. All mobile devices, whether county-owned or personally-owned, will also be remotely wiped of all business data if the user is no longer a County employee, or for the duration of any unpaid leave. This remote wipe will occur when the user is removed from the MDM system.

6. Devices whose users modify hardware or software installed to enforce security protocols (known as "jail-breaking", an action to replace or over-ride the device's native operating system or other security systems installed on the device), will not be allowed access to County technology resources.

7. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass these security systems will be deemed an intrusion attempt and could be dealt with in an appropriate manner.

8. All employees must remove County-specific data from mobile devices, whether County owned or personally owned, when such data are no longer required for performance of the employee's job duties.

HELP & SUPPORT

9. Le Sueur County supports technology that is used by its employees to conduct County business. However, Le Sueur County, through its Information Technology Department, reserves the right to establish and implement a system of prioritizing the allocation of resources for providing such help and support.

10. The Information Technology Department places the highest priority on providing support and help to users of County-owned mobile devices. The Information Technology Department places the next to highest priority on providing support and help to users of personally-owned devices that have been approved for business use. The lowest priority will be given to users of personally-owned mobile devices with only convenience-level access. Help and support for convenience access users will be limited to establishing connectivity to Le Sueur County's wireless networks and synchronization with Le Sueur County email and calendar system, as time allows.

11. Information Technology staff will maintain a list of mobile devices, both County-owned and personally-owned, for which the Information Technology Department is able to provide help and support. The Information Technology Department will provide help and support only in connection with devices that are County-owned or are personally-owned devices.

12. Mobile device malfunctions unrelated to connectivity to Le Sueur County technology resources on personally-owned mobile devices are addressed by the owner's service provider, not Le Sueur County Information Technology Department.

USER COMPLIANCE

Users who are authorized to bring their own device to work:

- Have no expectation of privacy for data contained on the portion of the device that is used for business purposes. All business-related messages and data transmitted through the County's technology resources are the property of Le Sueur County and are subject to being accessed, remotely deleted, or disclosed to Le Sueur County at all times and without notice.
- Have a high but not a guaranteed expectation of privacy for data contained on the portion of a personally-owned device that is used for personal purposes. Le Sueur County does not intend to intentionally access, delete or disclose data contained on the portion of the device that is used for personal purposes, unless directed to do so by the employee. However, it is possible that such access, deletion or disclosure may inadvertently or accidentally occur.

Employees that are issued a County-owned mobile device are prohibited from the following:

- Using the equipment for personal profit or gain.
- Using equipment to transmit, receive or distribute pornographic, obscene, abusive, or sexually explicit materials, or materials containing unclothed or partially unclothed people.
- Violating any local, state, or federal law or engaging in any type of illegal activity.
- Using the mobile device to engage in any type of harassment or discrimination, including but not limited to sexual harassment and harassment based upon race, gender, sex, sexual orientation, religion, national origin, marital status, status with respect to public assistance, disability or any other type of harassment or discrimination prohibited by law and County policy.
- Using the mobile device to engage in any type of commercial enterprise unrelated to the specific purposes and needs of Le Sueur County.
- Using the mobile device to engage in any form of solicitation.
- Using the mobile device to promote any political causes.

Whether using County-owned or personally-owned mobile devices to conduct County business, all users must cooperate with the staff in the Information Technology Department and the County Attorney's Office to preserve electronic records or data stored on the device that show the use of the device, and that are relevant to the

subjects of lawsuits or audits involving the County, its officials and employees. All mobile device users must immediately surrender the device for purposes described in this paragraph if requested to do so.

Users of County-owned or personally-owned mobile devices who seek access to County technology resources must confirm that they have read and understand this policy and must complete a training session about this policy. The training will include discussion of the responsibilities described in the user agreement. No user agreement will be accepted until the training is complete, and no access to County technology resources will be allowed without proof of a signed user agreement.

Disciplinary action for failure to comply with this policy
Employees failing to adhere to this policy may, at the full discretion of the employee's supervisor in consultation with IT, result in the suspension of any or all technology use and connectivity privileges. When violations of this Policy occur, County disciplinary procedures will be followed. If the employee is subject to a collective bargaining agreement, the disciplinary procedures in the agreement will be followed. Employee Relations staff must be consulted before any disciplinary action is taken based upon violations of this Policy.

Chair, Le Sueur County Board of Commissioners Date

Le Sueur County Administrator Date

Pricing Proposal
Quotation #: 9143426
Created On: 1/30/2015
Valid Until: 3/1/2015

County of Le Sueur MN

Scott Gerr
88 South Park Avenue
Le Center, MN 56057
United States
Phone: (507) 357-8286
Fax:
Email: sgerr@co.le-sueur.mn.us

Inside Account Executive

Anthony Favia
290 Davidson Avenue
Somerset, NJ 08873
Phone: 800-477-6479
Fax:
Email: Anthony_Favia@shi.com

All Prices are in US Dollar (USD)

	Product	Qty	Your Price	Total
1	AirWatch Green Management Suite Perpetual AirWatch - Part#: GMS-PL-DEV **Note:** License - One Time Fee	75	$38.67	$2,900.25
2	AirWatch Green Management Suite AirWatch - Part#: GMS-MF-DEV **Note:** Maintenance - Annual Fee	75	$9.94	$745.50
3	AirWatch Green Management Suite Basic On AirWatch - Part#: PS-GMS-OP-LITE **Note:** Premise Deployment Offering	1	$1,740.33	$1,740.33
			Subtotal	$5,386.08
			Total	$5,386.08

Additional Comments

If you are using SHI's contract# #48196 release C1046(5), please include this contract number on your PO
Please include billing and shipping in PO.

The Products offered under this proposal are subject to the SHI Return Policy posted at www.shi.com/returnpolicy, unless there is an existing agreement between SHI and the Customer.

Pricing Proposal
Quotation #: 9140498
Created On: 1/30/2015
Valid Until: 3/1/2015

County of Le Sueur MN

Scott Gerr
88 South Park Avenue
Le Center, MN 56057
United States
Phone: (507) 357-8286
Fax:
Email: sgerr@co.le-sueur.mn.us

Inside Account Executive

Anthony Favia
290 Davidson Avenue
Somerset, NJ 08873
Phone: 800-477-6479
Fax:
Email: Anthony_Favia@shi.com

All Prices are in US Dollar (USD)

	Product	Qty	Your Price	Total
1	AirWatch Green Management Suite Subscription License - Shared Cloud - Recurring 3 Year Fee AirWatch - Part#: GMS-SB-CLD-3USR-3Y **Note:** License -36 Months	50	$213.02	$10,651.00
2	AirWatch Green Management Suite Cloud Deployment Offering AirWatch - Part#: PS-GMS-CLD-SP **Note:** Professional Services - One Time	1	$1,491.71	$1,491.71
			Subtotal	$12,142.71
			Total	$12,142.71

Additional Comments

If you are using SHI's contract# #48196 release C1046(5), please include this contract number on your PO
Please include billing and shipping in PO.

The Products offered under this proposal are subject to the SHI Return Policy posted at www.shi.com/returnpolicy, unless there is an existing agreement between SHI and the Customer.

Pricing Proposal
Quotation #: 9140431
Created On: 1/30/2015
Valid Until: 3/1/2015

County of Le Sueur MN

Scott Gerr
88 South Park Avenue
Le Sueur, MN 56057
United States
Phone: (507) 357-8286
Fax:
Email: sgerr@co.le-sueur.mn.us

Inside Account Executive

Anthony Favia
290 Davidson Avenue
Somerset, NJ 08873
Phone: 800-477-6479
Fax:
Email: Anthony_Favia@shi.com

All Prices are in US Dollar (USD)

	Product	Qty	Your Price	Total
1	AirWatch Green Management Suite - Subscription License - Shared Cloud - Annual Fee AirWatch - Part#: GMS-SB-CLD-3USR-1Y **Note:** License - Subscription - 12 Month(s)	50	$78.90	$3,945.00
2	AirWatch Green Management Suite Cloud - Deployment Offering AirWatch - Part#: PS-GMS-CLD-SP **Note:** Professional Services - One Time Purchase	1	$1,491.71	$1,491.71
			Subtotal	$5,436.71
			Total	$5,436.71

Additional Comments

If you are using SHI's contract# #48196 release C1046(5), please include this contract number on your PO
Please include billing and shipping in PO.

The Products offered under this proposal are subject to the SHI Return Policy posted at www.shi.com/returnpolicy, unless there is an existing agreement between SHI and the Customer.