AGENDA ITEM or FINAL CONTRACT REVIEW SUBMITTAL FORM

AgendaTitle:
Draft Information Systems Acceptable Use Policy

Action Requested: Discussion

Parties to the Agreement:

Term Begins: **Term Ends:** **Grant Contract #:**

Summary:
We have updated the use policy to include use of personnel devices and cell phones.

Fiscal Impact: No direct fiscal impact.

Submitted by: Mike Lee **Submitter's Email Address:** mlee@gunnisoncounty.org

Finance Review: ○ Required ◉ Not Required

Comments:

Reviewed by: Discharge Date:

County Attorney Review: ◉ Required ○ Not Required

Comments:

Reviewed by: GUNCOUNTY1\atrezise Discharge Date: 2/5/2015 Certificate of Insurance Required Yes ○ No ◉

County Manager Review:

Comments:

Reviewed by: GUNCOUNTY1\mbirnie Discharge Date: 2/6/2015

○ Consent Agenda ○ Regular Agenda ◉ Worksession Time Allotted:

Agenda Date: 2/10/2015 Follow Up Agenda Date:

Revised April 2013

Gunnison County Government

Information Systems

Acceptable Use Policy

February~~July~~ 2015~~4~~

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who connect any device to Gunnison County networks, whether the device is County owned and assigned or personally owned. This Acceptable Use Policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet computers.
- Mobile/cellular phones.
- Smartphones.
- iPads
- PDAs
- Home or personal computers used to access County resources.
- Any device capable of storing County data and connecting to any ~~unmanaged~~ network not managed by Gunnison County.

Commented [JO1]: Needs to be defined

The policy applies to any hardware and related software that could be used to connect to county networks whether to access County resources or just the general Internet, even if said equipment isn't County sanctioned, owned, or supplied.

The overriding goal of this policy is to protect the integrity and security of the private and confidential client and business data that resides within Gunnison County's technology infrastructure as well as the network it runs on. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a device or carried over an insecure network where it can potentially be accessed by unsanctioned resources or individuals. A breach of this type could result in loss of information, damage to critical applications, poses risk and or damage to clients and constituents, creates liability for Gunnison County, and potential damage to the County's public image. Therefore, all users employing a device connected to Gunnison County's network must adhere to County-defined processes and policies for doing so.

Applicability

This policy applies to all Gunnison County employees, including full, part-time and seasonal staff, as well as, but not limited to, contractors, freelancers, and other agents who utilize either County-owned or personally-owned devices to access county networks to store, back up,

relocate or access any organization or client-specific data, as well as access the Internet. Such access to county networks is a privilege, not a right, and forms the basis of the trust Gunnison County has built with its constituents. Consequently, employment at or business with Gunnison County does not automatically guarantee the initial and ongoing ability to use these devices to gain access to County networks and information.

This policy addresses a range of threats to – or related to the use of – County networks including but not limited to:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive County data is deliberately stolen and sold.
Copyright	Software copied onto a device could violate licensing.
Malware	Viruses, Trojans, Worms, Spyware and other threats could be introduced via a device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the County to the risk of non-compliance with various identity theft and privacy laws. Further, use of unlicensed software exposes the county to potential non-compliance of license agreements.

Addition of new hardware, software, and/or related components to provide device connectivity will be managed as per this policy and by the Information Technology Department (IT). Non-sanctioned use of devices to back up, store, and otherwise access any County-related data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing with electronic use, data access, data storage, data movement, and connectivity to any element of the County network. To the extent this policy conflicts with any previously implemented policy dealing with electronic use, data storage, data movement, and connectivity to any element of the County network, this policy shall govern.

Commented [JO2]: Can be used as an insertion point for the Electronic Device Policy in Personnel Policy

Responsibilities

The Board of County Commissioners of the County of Gunnison has the overall responsibility for the confidentiality, integrity, and availability of County data and has delegated that responsibility to the County Manager through Board of County Commissioners of Gunnison County Resolution No.1983-20.

The Gunnison County Manager has in turn delegated the execution and maintenance of Information Technology and Information Systems to the Director of Information Technology Department.

~~The Board of County Commissioners of the County of Gunnison County has delegated the execution and maintenance of Information Technology and Information Systems to the Director of Information Technology Department.~~

Other IT staff under the direction of the Director of Information Technology Department are responsible for following and enforcing the procedures and policies recited herein.

All Gunnison County Government employees, and any third party granted access, are responsible to act in accordance with County policies and procedures.

Affected Technology

Connectivity of all devices will be centrally managed by Gunnison County Government's IT Department and will utilize authentication and strong encryption measures. Although the IT department is not able to directly manage external devices – such as home PCs – which may require connectivity to the County network, end users are expected to adhere to the same security protocols when connected to non-County equipment. Failure to do so may result in immediate suspension of all network access privileges so as to protect the County's infrastructure.

Policy and Appropriate Use

It is the responsibility of any employee of Gunnison County who uses a device to access County resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any device that is used to conduct Gunnison County business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules shall be observed:

Access Control

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect devices to County and County-connected infrastructure. IT will engage in such action if it reasonably believes such equipment is being used in a way that puts the County's systems, data, users, and clients at risk.

2. Each Department Head will be responsible for budgeting any potential costs associated with software required by IT to make personal devices compatible with Gunnison County's infrastructure, as well as any required security software.

3. ~~Prior to any device's initial use on the County network or related infrastructure,~~ ~~**all devices must be registered with IT and acquire management approval by completing a Technical Service Request (TSR).**~~ ~~TSR's will be automatically routed to the appropriate Department Head for review and possible approval, Requests from elected offices will be reviewed by the County Manager.~~ Gunnison County Government will maintain a list of approved devices and related software applications and utilities, and it will be stored on the County's Intranet at ~~_____.~~ www.gunnisoncounty.org//643/IT-Help-Information . Devices that are not on this list may ~~not~~ be connected to County infrastructure, with limited or no support from

Gunnison county IT department. If your preferred device does not appear on this list, contact the Help Desk at support@gunnisoncounty.org or 970-641-1410. ~~Although IT currently allows only listed devices to be connected to County infrastructure, it reserves the right to update this list in the future.~~

4. End users who wish to connect ~~such approved~~ devices to non-County network infrastructure to gain access to County data shall employ, for their devices and related infrastructure, an commercially available anti-virus system that is supported by vendor and virus definitions are upto date and current. ~~County-approved personal firewall~~ and/or any other security measure deemed necessary by the IT department. County data is not to be accessed on any hardware that fails to meet Gunnison County Government's established IT security standards.

5. All devices attempting to connect to the County network will be subject to monitoring and can expect to be inspected using technology managed by Gunnison County Government's IT department. All devices connecting to the County networks must have a device management application installed by IT staff to allow monitoring, remote wipe, remote password enforcement, tracking, etc. Authorized users with devices that have not been previously approved per this Acceptable Use Policy, or that are otherwise not in compliance with IT's security policies, or which represent any threat to the County network or data will not be allowed to connect, and should not connect to County networks.

6. Laptop computers or personal PCs may only access the County network and data using a Secure ~~Socket Layer (SSL)~~ Virtual Private Network (VPN) connection. The ~~SSL~~ VPN portal Web address will be provided to users as required ~~(or needed?)~~. Smart mobile devices will access the County network and data using similar secure mobile software installed on the device by IT or through secure web-sites~~.~~

7. Any content accessed via County networks are subject to Human Resources policies regarding content. All content accessed on County networks is to be for business purposes ~~only unless explicitly allowed per a TSR approved by a supervisor~~. Specific separate networks are provided with open content access. Examples of this ~~are Public Internet access on specific computers at county libraries, or via personal devices on WISC~~include the wireless access to a guest network.

Security

8. Employees using devices and related software for network and data access will, without exception, use secure data management procedures. All devices with appropriate capability must be protected by a strong password (County IT can supply the current definition~~), and all data stored on the device must be encrypted using strong encryption~~. See the ~~Gunnison County's~~IT department password policy for additional background. Employees agree to never disclose their passwords to anyone, particularly to family members if County work is conducted from home.

9. All users of devices connecting to County networks must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, ~~encryption,~~ and physical control of such devices (meaning any device used by someone other than the primary user reverts that device to an untrusted state). Any non-County computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by Gunnison County IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

10. It is prohibited to access Gunnison County data with any device that has had modifications to device hardware and/or OS software beyond routine installation of updates as directly provided by the applicable device maker or mobile operator, such as device "iOS Jailbreaking", "Android OS Rooting", or the equivalent.

11. Passwords and other confidential data as defined by Gunnison County's IT department are not to be stored unencrypted.

12. Any device that is being used to store Gunnison County data must adhere to the authentication requirements of Gunnison County's IT department. In addition, all hardware security configurations (personal or County-owned) must be pre-approved by Gunnison County's IT department before any county data-carrying device can be connected to it. This will include but is not limited to devices such as thumb drives, memory sticks, external drives, etc.

13. IT will manage and monitor security policies, network, application, and data access using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be monitored and will be deemed an intrusion attempt and will be dealt with in accordance with Gunnison County's overarching security policy.

14. Employees, contractors, and temporary staff will follow all County-sanctioned data removal procedures to permanently erase County-specific data from such devices once their use is no longer required and may be subject to County IT staff scrutiny to confirm a complete wipe of data is complete. ~~See County's Intranet at _____for detailed data wipe procedures for devices.~~

15. In the event a device is lost or stolen it is the absolute responsibility of the user to report this to IT immediately. Failure to do so can result in loss of privacy, use of any or all county IT resources, and possible legal action and/or reprimand. In such event, the device will be remotely wiped of all data and/or locked to prevent access by anyone other than IT. County IT is not responsible for any loss of data or costs associated with this action. If a county owned device is recovered, it can be submitted to County IT for re-provisioning.

16. Use Violations. No person shall use County communications systems to:

    a. Violate any municipal, county, state or federal law or regulation.

    b. Promote any commercial venture, political campaign, or personal purpose.

    c. Raise funds or engage in public relations activities that are not directly related to County business.

    d. Intentionally disrupt network or system use by others, either by introducing worms or viruses or by other means.

    e. Engage in any activities that could cause congestion and disruption of networks and systems, such as sending and forwarding chain letters, joining news subscription services, listening to music or watching video over the internet, and sending or receiving graphic or animation files not directly related to county business.

    f. Download copyrighted music, send or receive copyrighted materials, trade secret, proprietary financial information or similar materials without prior consent.

    ~~15.~~g. Transmit or, with foreknowledge, receive pornographic, racist, sexist or harassing material.

Formatted: Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

Purchases & Reimbursements

~~16.~~17. If an application vendor account is required on any County owned device, such as iTunes or Google Play, all accounts will be setup as an employee's personal account using their county login credentials (typically county assigned email address), with that employee's **~~personal~~ county purchasing/credit card** for any and all application or service purchases. ~~County~~

~~Purchasing Cards are NOT to be used unless approved by the department director or in the case of department director's the Assistant County Manager.~~

~~17.~~18. Only County assigned application installed on any device will be provisioned, distributed, and managed by County IT. Mobile Apps will be purchased via that employee's **county purchasing/credit card.**~~County IT and distributed, and eventually retrieved, via various management tools. This is the preferred method and any exceptions must be approved by County IT.~~

~~18.~~19. Employees ~~may be entitled to reimbursement for applications or services purchased with their personal credit card,~~must get ~~with~~ approval ~~o~~from their supervisor (e.g., voice usage, data usage, Wi-Fi hotspot usage, roaming usage, etc.) for any expense. ~~Standard expense reimbursement procedures shall be followed.~~

~~19.~~20. Non-business related services are not eligible for reimbursement, which may include SMS/MMS, ringtone downloads, 411 calls, or any other service not explicitly identified as eligible for reimbursement.

~~20.~~21. There are ~~no~~ specified caps on reimbursement amounts (e.g., in the form of fixed monthly stipends or maximum-expense limits, irrespective of charges incurred). Standard expense reimbursement procedures established by the Finance Office shall be followed.

~~21.~~22. Replacement cost for County devices ~~out of warranty when~~ damaged or lost due to employee negligence will be the responsibility of the employee.

Help & Support

~~22.~~23. Gunnison County Government's IT department will support its sanctioned hardware and software, but is not responsible for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT department. If conflicts or problems arise, the IT department will wipe and/or reset the device to factory settings. If county owned, the device will be restored only with an approved configuration using authorized applications. If not county owned, the device restoration is the responsibility of the owner and any loss of data, configuration, and or applications is not the responsibility of County IT. County IT will not provide or maintain data or setting configuration backups of any device.

~~23.~~24. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the County network.

Organizational Protocol

~~24.~~25. IT can and will establish audit trails and these will be accessed, published and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to Gunnison County Government's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains Gunnison County Government's highest priority.

~~25.~~26. The end user agrees to immediately report to his/her manager and Gunnison County Government's IT department any incident or suspected incidents of unauthorized data access,

data loss, and/or disclosure of County resources, databases, networks, etc., and assist with any investigation. Security is everyone's responsibility.

~~26.~~27. Every device user will receive IT training covering this policy, security, County IT resource use. While a device user will not be granted access to County resources using a device without completing training and accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents, and no access will be granted.

~~27.~~28. Any questions relating to this policy should be directed to the Information Technology Systems Director via the IT Help Desk at ~~970-453-3510~~ 970-641-1410.~~4140 or _____~~.

Policy Non-Compliance

Failure to comply with the Information Systems Acceptable Use Policy may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

The (i) County Manager, (ii) ~~Assistant~~ Deputy County Manager, and (iii) immediate Manager or Director will be advised of breaches of this policy and will be responsible for appropriate remedial action which may include disciplinary action, including suspension or termination of employment.

Employee Declaration

I, _____, have read and understand the above Information Systems Acceptable Use Policy, and consent to adhere to the rules outlined therein.

_____	_____
Employee	Date
_____	_____
Department Head or Asst County Manager	Date
_____	_____
IT Administrator	Date