County Systems & Network Guidelines for SCORE Access

# Purpose

These guidelines are meant to help counties meet Federal, State, and Local SCORE systems security requirements. Under each heading are questions that the county must use to analyze their network security. A county has a security problem if the county cannot answer a question or cannot provide an affirmative answer to the question. A county must work with their information technology department to remedy an existing problem.

# General

* Do you have an inventory of all devices permitted to connect to the SCORE network?
* Have you performed a site survey to determine what areas within the area need coverage?
  + - Are monitors displaying sensitive information blocked from view by the public?
    - Are network ports, network equipment, or other systems in non-monitored areas restricted from access by the public?
* Have users been trained to never post or store passwords, grid cards, wireless keys, or other sensitive information on or around work areas or workstations?
* Are user work areas audited and monitored to prevent users from posting sensitive information?
* Do all system changes go through a County IT management change approval process?
* Are proper security controls in place to monitor physical access to SCORE systems?
  + - Do you have staff monitoring, cameras, locks, or other controls needed to ensure only authorized personnel can access networks and systems?
* Are all authorized staff required to wear identification, such as a government issued photo ID badge, to clearly distinguish between onsite personnel and public visitors?

# Network

* Are all network devices including firewalls, routers, and switches configured according to industry best practices?
* Is there documentation and business justification for use of all services, protocols, and ports allowed?
* Are firewall and router rule sets reviewed at least every six months?
* Are network ports and/or wall jacks monitored and/or restricted from public or other non-county related use?
* Is access permitted to only known trusted DNS servers?
* Is there an up to date network diagram including any wireless networks?
* Are vendor supplied defaults for simple network management protocol (SNMP) community strings and passwords changed?
* Is all non-console administrative access encrypted using technologies such as SSH, VPN, or SSL/TLS?
* Is all network equipment configured to keep accurate time synchronization with a trusted NTP time source?

# Wireless Networks

* Do you ensure that all wireless access points are managed by either the State or Counties?
* Do you ensure that all wireless access points are physically secure and not physically accessible by the public?
* Do you ensure that all wireless traffic utilizes at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection?
* Do you disable peer-to-peer wireless network capabilities on wireless clients?
* Do you disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need?
* Do you configure all wireless clients used to access private networks or handle organization data in such a way that they cannot be used to connect to public wireless networks or any other networks beyond those secured and controlled by either the State or County?
* Do you ensure that wireless keys and network information isn’t shared with staff or others that don’t need to know?
  + - Do you document all staff that has access to a wireless key or other network information?
* Are wireless passwords and pass phrases changed at least every three months and every time someone with access to the password or pass phrase leaves County or State employment?

# MiFi Networks - Cell Phones and Mobile Device Hot Spots or Cards

* Are vendor supplied default passwords and PSK passphrases changed to meet wireless network minimum requirements? Vendor supplied default should never be used!
* If a wireless “Hot Spot” is utilized on a MiFi device are all the wireless network requirements above being implemented?
* Are mobile devices being utilized for MiFi access secured with at least a 15 character passcode meeting password complexity requirements to prevent un-authorized access?

# Client Systems – County Workstations

* Do you have an inventory of permitted software applications on client systems?
* Are only software packages needed to perform business related functions being installed?
* Are basic users given non-administrator accounts with no rights to install software on client systems?
* Do client systems have up-to-date anti-virus installed with real time scanning enabled?
* Do client systems have advanced malware protection with forensics logging enabled?
* Do client systems have a software firewall installed, configured and enabled?
* Are users restricted from disabling anti-virus and firewall software?
* Do you run a vulnerability scan on client systems? Are vulnerability scans completed on a regular basis or whenever significant changes occur on systems?
* Are all client systems configured securely according to industry best practices?
* Are local administrator privileges controlled and only used when necessary on client systems?
* Are all systems patched with updated operating system and third-party security patches?
* Is any sensitive SCORE data downloaded from the system only stored on securely encrypted drives or devices?
* Do client systems have proper security logging enabled to identify user authentication events, accurate date and time, successful and failure events?
* Are client systems configured to keep an accurate time with a trusted NTP time source?

# User Training & Requirements

* Have users reviewed and signed the SCORE Acceptable Use Policy?
* Have users been informed to never share passwords or grid card information?
* Are all users given a unique username before allowing them access to SCORE?
* Are all users required to use a multifactor authentication device such as a grid card or token?
* Are users trained on complex password requirements in the AUP?

|  |  |
| --- | --- |
| * At least 15 characters * Lower-case letter * Number | * Upper-case letter * Symbol |

* Are users trained on whom to contact if they are experiencing unusual workstation activity?
* Have all County User Administrators completed the Securing the Human course provided by the Colorado Department of State?
* Are users trained to never install software or browse the Internet on SCORE client systems?
* If a user session is idle for more than 15 minutes is the user required to re-authenticate or un-lock their workstation?

# Resources for Counties

1. CIS Handbook for Elections Infrastructure Security

<https://www.cisecurity.org/elections-resources/>

1. Multi-State Information Sharing and Analysis Center Services

[https:/www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf](https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf)

1. Center for Internet Security Hardening Guides

<https://www.cisecurity.org/cis-benchmarks/>

1. Critical Security Controls

<https://www.cisecurity.org/controls/>

1. Online File Malware Checker

[www.virustotal.com](http://www.virustotal.com)

1. NIST – National Institute of Standards and Technology Publications

<http://csrc.nist.gov/publications/PubsSPs.html>