MARICOPA COUNTY SHERIFF'S OFFICE POLICY AND PROCEDURES

Subject	Policy Number
EMPLOYEE ACCESS TO THE INTERNET/INTRANET	**GD-23**
	Effective Date **08-28-18**

Related Information	Supersedes
County Policy A1609, Acceptable Use of County Technology Resources County Policy HR2409, Teleworking CP-2, *Code of Conduct* GF-3, *Criminal History Record Information and Public Records* GM-1, *Electronic Communications and Voice Mail*	GD-23 (05-30-13)

PURPOSE

The purpose of this Office Policy is to establish general procedures for employee use of the Internet, Intranet, and Office technology resources.

POLICY

It is the policy of the Office to ensure that guidelines are in place for the proper use and security of Office technology and Maricopa County resources to comply with all applicable laws, rules, and regulations.

DEFINITIONS

Data Loss Prevention* (DLP)*: Implementation of protective measures to prevent sensitive data information from being released outside the organization.

Internet: A worldwide publicly accessible system of interconnected computer networks.

Intranet: The generic term for a collection of private computer networks within an organization that uses network technologies as a tool to facilitate communication, between people or work groups, to improve the data sharing capability and overall knowledge base of an organization's employees.

Local Agency Security Officer* (LASO)*: An employee within the Office serving as the technical contact and liaison with the State Information Security Officer. The LASO will advise and assist the System Security Officer (SSO) with compliance with all Arizona Criminal Justice Information Systems (ACJIS) and FBI CJIS policies and procedures.

Mobile Data Computer* (MDC)*: A computerized terminal device used in sheriff's vehicles to communicate with a central dispatch office. MDCs feature a screen on which to view information and a keyboard or keypad for entering information.

Sensitive Data Information: Data or information that is personally identifiable or should otherwise be considered confidential. Examples include social security numbers; driver license information; credit card/banking information; usernames and passwords; network information or schematics; investigative information, including data derived from state and federal sources; Computer Aided Dispatch (CAD); Records Management System (RMS); Jail Management System (JMS); and health care/Health Insurance Portability and Accountability Act (HIPAA).

***System Security Officer* (SSO):** An employee within the Office responsible for ensuring Office personnel are in compliance with all applicable laws, rules, regulations, policies, and procedures governing the Arizona Criminal Justice Information Systems (ACJIS) or Criminal Justice Information Services (CJIS) networks.

***Virtual Private Network* (VPN):** A technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. It provides varying levels of security so that traffic sent through the connection stays isolated from other computers on the intermediate network, either through the use of a dedicated connection from one end of the VPN to the other, or through encryption. It can connect individual users to a remote network or connect multiple networks together.

Web Proxy: A network device that accepts and responds to requests for external websites. The web proxy also applies filtering policies, which allows or blocks access to sites, and logs all user activity.

PROCEDURES

1. **Authorization:**

   A. Employees are provided access to Internet resources automatically; however, a web proxy filtering policy is applied. The web proxy filter blocks access to known malicious websites, websites categorized as adult or otherwise inappropriate, and websites that consume large amounts of network bandwidth such as streaming video, audio, and social networking. Streaming video and audio websites are disruptive to the Maricopa County network and should be used sparingly, as required per assignment. Additionally, websites that allow information to be stored online, such as Dropbox, OneDrive and Google Drive, are also blocked by default as a Data Loss Prevention (DLP) measure. Online storage websites are not considered to be safe locations to store or share Office information.

   B. An unrestricted filtering policy should be applied, by default, to personnel in any investigative role, as well as personnel in other Office divisions that have received approval for such access through their chain of command. The request and approvals shall be forwarded to the Technology Bureau Help Desk, and a service ticket shall be created. The Technology Bureau Infrastructure and Security Division will review and implement the request. Unrestricted access to websites that are otherwise blocked, especially those that are disruptive to the Maricopa County network, should only occur while performing official Office duties.

   C. Other filtering policies are available and may be applied as requested on a case-by-case basis. The policy can apply to a specific user or computer. These include:

      1. Restricted Policy: Blocks all outbound internet requests.

      2. Default Policy – Streaming Media: Allows streaming media to include, but not limited to, YouTube, Pandora, etc.

      3. Default Policy – Online Storage: Allows online storage to include, but not limited to, Dropbox, OneDrive, etc.

      4. Default Policy – Social Networking: Allow social networking to include, but not limited to, Facebook, Twitter, etc.

2. **Accessibility:**

A. Employees are restricted from using personal electronic devices to directly access the Office's secured network. VPN connectivity, using a personal device, is allowed on an individual basis with written supervisory approval. Employees using VPN connectivity shall adhere to Office Policy and Maricopa County Policy A1609, Acceptable Use of County Technology Resources.

B. Internet and Intranet access shall be used for routine Office business. However, employees may make limited use of the Internet and Intranet under the following circumstances:

1. Scheduling of personal appointments, as an effective extension of overall time management;

2. Sharing of event driven information and planning of work-related social events where the intent is to enhance employee morale; or

3. Other limited uses that are not disruptive to other personnel or to the network overall, offensive to others, harmful to morale, or solicitous of others for a non-work-related activity.

3. **Conduct:** While using the Internet and Intranet, employees shall conduct themselves in a manner which reflects favorably on both the Office and the Maricopa County, as specified in Office Policy CP-2, *Code of Conduct* and applicable Maricopa County policies.

4. **Restricted Sites:** Internet sites which contain sexual content, solicit or encourage illegal activities, or disparage an individual's race, gender, religion, color, national origin, age, disability, or sexual orientation shall not knowingly be accessed, except while acting under lawful and specific orders from a supervisor.

5. **Social Networking Sites:** Social networking sites shall not be accessed on Office equipment while on duty, unless in the performance of official duties, as specified in Office Policy CP-2, *Code of Conduct*. Examples of social networking sites include Facebook, Twitter, Instagram, and Pinterest.

6. **Usage Audits:**

A. The Technology Bureau logs and audits employee's use of the Internet and Intranet. This includes monitoring sites visited, information accessed, network bandwidth consumed, and the dates and times of these activities. Employees using Office technology resources shall have no expectation of privacy in the use of these tools or any content therein.

B. Supervisors may request usage reports for specific users by submitting a request through the MCSO Help Desk.

7. **Personal E-mail Access:** Employees are authorized limited use of personal internet-based e-mail, as specified in Office Policies CP-2, *Code of Conduct* and GM-1, *Electronic Communications and Voice Mail.* Personal e-mail shall not be used to conduct official Office business, or to communicate or store/backup any sensitive data information, to include network accounts, passwords, investigative or application-specific information. Examples of personal internet-based email services include Yahoo Mail, Gmail, and Outlook/Hotmail.com.

8. **Secondary Dissemination:** Employees are responsible for the confidentiality of all information accessed or transmitted during their duties, including criminal history record information, as specified in Office Policy GF-3, *Criminal History Record Information and Public Records*.

9. **Alternate Networks:** VPN usage to gain access to the Intranet or Maricopa County technology resources are subject to this Office Policy, Maricopa County Policy HR2409, Teleworking and Maricopa County Policy A1609, Acceptable Use of County Technology Resources.

10. **Mobile Data Computer (MDC)**: Employees who utilize data usage on MDC laptops must be especially aware of network and data usage. Internet connectivity for the MDCs traverses the MCSO network and uses data and bandwidth over the wireless carrier network. Internet usage from MDCs, specifically streaming video and audio, shall only be used in the performance of official duties. Additionally, the viewing of body-worn camera videos on evidence.com is allowed but uploading of body-worn camera video through the MDC is prohibited.