MARICOPA COUNTY SHERIFF'S OFFICE POLICY AND PROCEDURES

Subject	Policy Number
EMPLOYEE ACCESS TO THE INTERNET/INTRANET	**GD-23**
	Effective Date **04-08-25**

Related Information	Supersedes
CP-2, *Code of Conduct* GD-7, *Media Relations and Social Media* GF-3, *Criminal History Record Information and Public Records* GM-1, *Electronic Communications, Data and Voice Mail* Maricopa County Policy A2611, Use of County Technology Resources Maricopa County Policy HR2409, Teleworking	GD-23 (08-28-18)

PURPOSE

The purpose of this Office Policy is to establish guidelines and 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

Business Continuity Plan* (BCP)*: A plan created to offer up steps to recover or maintain operations to business functions during a disaster situation.

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, and to improve the data sharing capability and overall knowledge base of an organization's employees.

Mobile Data Computer* (MDC)*: A computerized terminal device used in Office 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.

Phishing: The fraudulent practice of sending electronic mail, redirecting personnel to a compromised website, or other messages purporting to be from a reputable source to induce an employee to reveal personal information such as username and passwords.

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); Sheriff's Inmate Electronic Data SHIELD; and health care/Health Insurance Portability and Accountability Act (HIPAA).

Virtual Desktop Infrastructure* (VDI)*: A virtualized desktop hosted on a secure server located in a Maricopa County Sheriff's Office (MCSO) defined datacenter. Access to VDI is accomplished through a secure network to an endpoint device and/or application to retain all data in an MCSO controlled system.

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:** Employees are provided access to Internet resources automatically; however, a web proxy filtering type 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.

    A. Streaming video and audio websites are disruptive to the Maricopa County network and should be used sparingly, as required per assignment. Websites that allow information to be stored online, such as Dropbox, 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. The default filtering type policy applied to all personnel shall be the Default Policy – Streaming Media. If Office personnel need a less restrictive default filtering type policy they will need approval for such access through their chain of command. The request and approvals shall be forwarded to the Technology Management Bureau, MCSO Operations Center, and a service ticket shall be created. If approved, the Technology Management Bureau Infrastructure and Security Division shall implement the request. Access to websites that are otherwise blocked, and are disruptive to the Maricopa County network, should only occur while performing official Office duties.

    C. Office divisions requesting an unrestricted filtering type policy, which allows access to internet or social media applications not normally accessible to perform their official duties, such as law enforcement investigative divisions or the Professional Standards Bureau, may receive a filtering type policy applied as requested through their division commander or designee to the Technology Management Bureau Infrastructure and Security Division on a case-by-case basis. The filtering type policy can apply to a specific user or computer which includes:

        1. Restricted Policy: Blocks all outbound internet requests.

        2. Default Policy – Streaming Media: Allows streaming media to include, but not limited to, YouTube.
        3. Default Policy – Social Networking: Allow social networking to include, but not limited to, Facebook, X formally known as Twitter, etc.

4. Net Motion Policy Default Streaming: Policy used only by personnel required to connect through net motion.

5. Net Motion Policy Unrestricted: Policy used only by personnel required to connect through net motion with no filtering to conduct investigative analysis. This filtering type policy is audited by IT governance and is used to determine if personnel are required to be in an unrestricted category.

6. TrainingLAB Policy (Kiosks): Policy used in the training labs to minimize internet sites.

7. Tech Bureau Unrestricted Policy: In use by the Technology Management Bureau for troubleshooting and research. This filtering type policy is audited by IT governance and will determine if personnel require to be in an unrestricted category.

8. Pre-employment Policy (Kiosks): Policy used for kiosks systems used in pre-employment to limit internet sites.

2. **Accessibility:**

A. Employees are restricted from using personal electronic devices to directly access the Office's secured network. Connectivity shall adhere to Office Policy and Maricopa County Policy A2611, Use of County Technology Resources. Personal electronic devices may be authorized to access the Virtual Desktop Infrastructure (VDI) in the event of a Business Continuity Plan (BCP) situation or with written approval from Technology Management Bureau command personnel.

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 Internet 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. **Restricted Activities:** Utilizing other employee or services accounts IDs and passwords is strictly prohibited. Employees shall not knowingly attempt to bypass their filtering type policy for obscure internet usage. Online content or applications that require IDs and passwords should not be used by employees without prior authorization from the Technology Management Bureau. Approved applications should be routed through the OKTA, user authentication and identity control software and any other requests for a

username and password should be considered as a phishing attempt and reported to the Technology Management Bureau.

6. **Internet and Social Media/Networking Sites:** Social networking sites may be authorized for viewing Office related social media content. Examples of social networking sites may include, but are not limited to, Facebook, X formally known as Twitter, Instagram, and Pinterest. Office employees shall abide by the provisions for internet and social media use as follows:

   A. Content shall not be accessed on Office equipment unless in the performance of official duties or accessing Office controlled social media sites for viewing purposes, as specified in Office Policy CP-2, *Code of Conduct*.

   B. Any internet and social media/networking sites deemed to create a potential security and privacy risk to the Office network and the systems and data the Office is charged with protecting shall be restricted by the Office, unless otherwise specified in this Office Policy.

   C. Internet and social media/networking sites, such as Tik Tok, shall not be accessed on Office equipment that is otherwise banned as a result of an Office, or Maricopa County Board of Supervisors, or Governor of the State of Arizona, or US Federal Government directive and/or law, unless otherwise specified in this Office Policy.

   D. Further details regarding social networking sites are specified in this Office Policy and Office Policy GD-7, *Media Relations, and Social Media*.

7. **Usage Audits:** The Technology Management Bureau logs and audits employees' use of the Internet and Intranet which includes monitoring sites visited, information accessed, network bandwidth consumed, and the dates and times of these activities.

   A. 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 Operations Center.

8. **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, Data, 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 e-mail services include Yahoo Mail, Gmail, and Outlook/Hotmail.com.

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

10. **Alternate Networks:** Virtual Private Network (VPN) usage to gain access to the Intranet or Maricopa County technology resources are subject to this Office Policy and Maricopa County Policy HR2409, Teleworking.

11. **Mobile Data Computer (MDC) and Hot Spots**: Employees who utilize data usage on MDC laptops or through an Office-issued hotspot device either on a cellular phone or independent device must be aware of network and data usage. Internet connectivity for these devices traverses the Office's network and uses data

and bandwidth over the wireless carrier network. Internet usage from MDCs and hot spots, specifically streaming video and audio, shall only be used in the performance of official duties. MDCs may be used for uploading body-worn camera videos through the appropriate Office application to evidence.com.