5750 Duluth Street
Golden Valley, Minnesota 55422-4036
763.543.2600

Benefits through membership, sharing, and collaboration

Member Security Policy 2024

December 1, 2023

Section 1 – Security Policy Introduction

Section 2 – Password Management

Section 3 – Physical Security

Section 4 – General Management

Section 1 – Security Policy Introduction

Purpose:

This document outlines LOGIS member security requirements and recommendations. This document was created by LOGIS and our membership and is reviewed annually.

The purpose of the LOGIS Member Security Policy is to set standards for security to help protect LOGIS and our members from unnecessary business interruption and unauthorized and/or inappropriate access. The association recognizes that our organizations share common systems and infrastructure and it is in everyones best interest to assure security standards are established for the common good of all members.

This policy outlines requirements that must be ahered to by our member organizations for administration and security. We recommend each organization incorporate any items which apply to end users into their own IT policy.

Enforcement:

LOGIS will work with each member organization to address, implement and troubleshoot problems related to security. LOGIS maintains the right to discontinue service to any member that is adversely affecting the security or performance of LOGIS or other member organizations systems, until such time as the member's problem is rectified.

In the event LOGIS discontinues service, LOGIS will immediately notify the member's IT staff and work with the member's staff to rectify the problem.

Violations of the LOGIS Members Security Policy will be reported to the member organization in the following order:

- A letter will be sent from LOGIS detailing the policy violation, corrective action, and timeframes, to the member's IT manager or responsible party.
- If the timeframe has expired from the first notification and the violation has not been corrected, a second notification will be sent from the LOGIS Executive Director to the organization's executive manager/administrator detailing the policy violation, corrective action, time frames and ramifications if failure to comply.

Administration:

LOGIS's Director of Infrastructure & Shared Services is responsible for maintaining and administrating the LOGIS Members Security Policy and reviewing member compliancy.

Section 2 – Password Management

Purpose:

The purpose of this section is to establish a standard on password management. The following sub-sections outline the requirements of password management.

Requirements for Password Management:

Users: All passwords are to be treated as confidential. Employees and contractors must keep their passwords confidential and not share them with anyone that is not authorized.

All system and user level passwords must:

1) Adhere to the following:
   - Must be a minimum of twelve characters in length.
   - Must be a minimum of fifteen characters in length for local non-domain Windows passwords.
   - Must be changed from the default on new software and equipment.
   - Must be changed every 90-days.
   - Have a digit, symbol character, one upper case and one lower case letters, for example: kep1tSafe#
   - Have not been previously used in the last twenty-four password rotations.
   - Password policies must be defined on the operating system level.
   - Failed authentication attempts must be logged.
   - Passwords used for accounts in the Member or LOGIS networks must be different than passwords used elsewhere (e.g. personal bank accounts, personal email accounts, etc.).
   - Must be changed by the user on first use.

   A pass phrase may be used in place of a password but must be a minimum twelve characters long and conform to the other password requirements. An example of a pass phrase is "The:(TrafficOnThe101was?ThisMorning". Protected service accounts with a long unrecorded password or passphrase are exempt from the password change requirement.

OR

2) Utilize a Multi-factor Authentication (MFA) software login.

OR

3) Follow CJIS Security Policy 5.9.2, 5.6.2.1.1.2, Advanced Password Standards. https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center

Members must notify LOGIS immediately upon separation of relevant employees and contractors so their LOGIS accounts can be disabled.

Members must conduct, at a minimum, an annual audit of all accounts to ensure inactive accounts have been disabled or deleted.

Network Equipment: All network equipment (switches, routers, firewalls) must utilize passwords. A password is required for configuration access. The network equipment includes all network hardware utilized to connect to the member or LOGIS.

Note: The State MNIT group or LOGIS manage state router configurations. State router configuration access is through the State two-factor authentication service using tokens issued by the State to select Network Services staff.

Database Access and Database Password Management: All SQL database users must have passwords defined. All DBA user passwords must conform to the system-level password requirements. All DBA passwords are only to be known by the IT staff and DBAs. Database administrators must have separate users and passwords defined for tracking purposes.

All client database users' passwords must conform to the previously listed password requirements.

SNMP: SNMP (Simple Network Management Protocol) is used on all network devices for monitoring of resources and preventative maintenance. Community strings serve as access passwords in SNMP. The following is a list of procedures regarding the management of this resource:

- Community strings must conform to the system-level password requirements, except as listed below.
- Community strings must be different from the passwords used to log in to the devices.
- Read Only and Read+ Write community strings must be different if the Read Only community strings are distributed to outside organizations.
- A keyed hash must be used where available (e.g., SNMPv3).
- SNMPv2 or higher shall be used
- Community strings must be changed on a yearly basis or upon separation of an IT staff member.
- SNMP access must be configured to only devices that do the monitoring on the network.
- The SNMP service should be configured to only accept connections from IT or authorized SNMP management devices.

VPN: VPN (Virtual Private Network) has been established for LOGIS and many of our members. The following is a list of procedures regarding the management of this resource:

- VPN access to the LOGIS networks via remote access is to be controlled using a domain user/password authentication or approved two-factor method such as a hardware or software token.
- No authorized user shall give out their VPN authentication credentials to any other person. However, logged temporary tokens may be set up by the Member's IT department if needed.
- Every member is responsible for specifying the access level and the frequency of password changes for their remote users.
- VPN users must be configured to use two-factor ("advanced") authentication rather than domain passwords for authentication to police segments outside of a secure police building or squad car.

Applications: Where possible, in-house developed and third-party applications should adhere to these password requirements.

Optional Recommendations for Password Management:

The following are optional recommendations for password management. This sub-section is not a requirement. All passwords should follow these specifications:

- Be a minimum of fifteen characters in length.
- All system and user passwords (e.g., root, enable, NT administrator) should be changed immediately with the separation of an IT staff or LOGIS employee.
- Should not be a word in any language, slang, dialect, jargon, etc.

- Should not be a word followed or proceeded only by a number and/or symbol
- Should not be a word with just a similar looking number in place of a letter, e.g. s=5, i=1.
- Should not be based on personal information, names of family, etc.
- Should not be similar to one previously used
- Should not be written down
- Should not be stored electronically without being encrypted, and is not recommended for normal users.

Examples of stronger passwords that are harder for password dictionary cracking programs to guess, but based off easy to remember terms include: C@ts-and-Dogs-Living-together and i7ovemydog!!

Use of Generic users and passwords is strongly discouraged. Auditing of network resources depends on user names and passwords. Generic users limit the effectiveness of the auditing.

Local workstation administrator accounts should use a different password than the domain administrator and local server administrator accounts. Physical access to a workstation could lead to disclosure or recovery of a local workstation password by an unauthorized person, which could otherwise lead to compromise of a server if the same password is used.

Local passwords on Cisco network equipment should be stored using type 5 (MD5) encryption rather than type 7 (reversible) where possible.

Passwords should be transmitted in encrypted form over the network.

Passwords should not be stored in web browsers such as Chrome and Edge. Recommend the option be disabled using Group Policy.

Password should be stored in an organization hosted and managed password vault or Privileged Access Management (PAM) tool.

Optional Recommendations for Screen Lock:

The following are optional recommendations for screen lock. This sub-section is not a requirement.

- Screen lock set to 15 minutes or less
- Authentication set to unlock
- Auto-logoff set for shared workstations or kiosks
- When stepping away from computer, screen lock should be manually forced

Section 3 – Physical Security

Purpose:

The purpose of this section is to establish the rules for the granting control, monitoring, and physical access to the IT facility. The controlling of physical access to the members' IT rooms and data closets are extremely important to the overall security.

Requirements for Physical Security:

All servers and network communication equipment (switches, routers, and firewalls) will be locked in a physical cabinet or located in a secured room with access restricted to only IT staff and authorized employees. Any non-employee access that is approved must be accompanied and supervised by an authorized employee.

Public Access on the Members or LOGIS Network:

In limited cases, public access computers or terminals can be provided. Any public access computers or terminals must be located on a separate network segment with limited access to the member or LOGIS networks. These devices must be supervised and locked down to a limited scope of functions or access. No unsupervised public access computers or terminals can be connected to the LOGIS or member's network.

Optional Recommendations for Physical Security:

The following are optional recommendations for physical security. This sub-section is not a requirement.

LOGIS recommends members install access control systems that take advantage of card readers that allow simplified employees access management to facilities and log and record employee access. In highly secure areas these access readers should incorporate Multi-factor Authentication (MFA) access readers (e.g. IT computer rooms, evidence rooms, etc.)

All network communication (local and wide area network), fiber termination, and data termination should be located in the data communications rooms. Access to these rooms should be restricted to IT staff, LOGIS, and optionally the building supervisor if appropriate.

All access to these locations should be logged and recorded.

Areas of buildings open to the general public should have any open network ports disabled or use another method of preventing unauthorized access to the city network. Wi-Fi access points in public areas should not be easily physically accessible by the public. Network monitoring should be installed at the member's network that will notify and alert the IT staff in the event of new devices and sniffers being installed on the network.

Police background checks are strongly encouraged on all people having access to the systems.

Locking screen savers and shredders are recommended for off-site staff environments.

A set of recent backup media should be securely stored off-site for disaster recovery purposes.

Section 4 – General Management

Purpose:

The purpose of this section is to provide a secure network infrastructure for LOGIS and our members.

Windows Security:

Purpose of Windows Security: The purpose of Windows Security is to advise the members of procedures to secure their servers, workstations, and networks, and applies to all Windows systems accessing the member's network.

Requirements for Windows Security:

1. Rename the administrator account.
2. Setup domain policy to have a minimum of the following:
    a. Account lockout threshold after 5 invalid attempts.
    b. Account lockout duration 30 minutes.
3. Install all critical security patches within three weeks of release date.
    a. Critical security patches that fail installation, fail testing or cause system issues must be analyzed for root cause, with the patches applied promptly or compensating controls put in place.
4. Install all other security patches within four weeks of release date.
    a. All other security patches that fail installation, fail testing or cause system issues must be analyzed for root cause, with the patches applied promptly or compensating controls put in place.
5. Disable storage of passwords in the weaker LANMAN format.
6. Physically sanitize of destroy media or server hard drives that contain confidential or highly sensitive data per the NIST 800-88 standard.
7. Operate under vendor supported operating system and applications versions.
8. Enable auditing of the following successful and failed events, tuned to be able to retain logs for a day or more.
    a. Logon/logoff
    b. Account management
    c. Policy changes
    d. System events
    e. File share initial access
9. Bureau of Criminal Apprehension (BCA) requirements for systems that store, process or transmit Criminal Justice Information (CJI) (MNJIS-5002-CJDN-Network-Security-Policy).
    a. Critical – Remediate within 7 days. These vulnerabilities pose the highest risk to applications, systems, and agency data.
    b. High – Remediate within 30 days. These vulnerabilities pose a significant risk to applications, systems, and agency data.
    c. Medium– Remediate within 90 days. These vulnerabilities pose a moderate to indirect risk to applications, systems, and agency data.
    d. Low – Remediate during the next routine system maintenance. These vulnerabilities only expose noncritical system information.

Optional Recommendations for Windows Security:

1. Disable GUEST account access in domain policy.
2. Setup hidden shares when possible.
3. Setup group access to directories and remove access to the groups of EVERYONE, DOMAIN USERS.
4. Mobile devices containing confidential information should use whole-disk encryption
    a. Whole disk encryption should use pre-boot authentication

5. Setup a login banner to clarify that access to the system is for authorized users only and may be monitored.
6. Disable or rename the default Admin$, C$ and D$ shares when possible.
7. Use Center for Internet Security (CIS) operating system hardening guidelines.
8. Install all security patches within two weeks of release date.
9. Track and update non-Microsoft user applications when security patches are released.
10. Enable the Windows or third-party firewall to block unexpected incoming traffic
11. Purge workstation magnetic hard drives by overwriting all disk space with binary zeros or random data (not just formatting), using a drive's internal whole-disk Secure Erase function, or degaussing.
12. Purge solid state drives by overwriting all disk space twice with binary zeros or random data (not just formatting), or physically destroy.
13. Only grant administrator rights access to users who require it to perform their job functions.
14. Disable inactive user accounts which have not been used in over 90 days, unless required.
15. Disable vulnerable cryptographic protocols (SSLv2, SSLv3, TLS 1.0, TLS 1.1) on servers.
16. Configure RDP on server: Force NLA and/or Digital Certificate signed by member Certificate Authority, set encryption to High.
17. Remove "Anonymous Logon" from the Active Directory "Pre-Windows 2000 Compatible Access" group, to help limit Active Directory read access to internal users.
18. Limit domain admin accounts by having separate user accounts with domain admin for IT staff and assigning service accounts local admin access only to the servers they need admin access on.

Change Management:

Purpose of Change Management: The purpose of change management is to control the lifecycle of all changes, enabling beneficial change to be made with minimum disruption to IT services.

Optional Recommendations for Change Management: A change management procedure shall be utilized in order to make authorized changes to the member's network environment. This procedure shall include documentation and formal approval of all changes. These items include, but not limited to, firewalls, routers, network switches, wireless controllers, access points, security appliances, directory services, servers, virtualization environments, storage devices (e.g. SANS), Voice over Internet Protocol (VoIP) systems, computers, squad computers, mobile devices, and smartphones.

Virtual Server Security:

Purpose of Virtual Server Security: The purpose of Virtual Server Security is to advise the members of procedures and practices to secure their virtual server environments from unwanted access.

Optional Recommendations for Virtual Server Security:

1. Utilize isolated physical servers to separate DMZ and internal virtual servers,
2. Utilize isolated VLANs on DMZ servers versus internal servers. This includes network segments such as VMWare fault tolerance, vMotion, load balancing, etc.
3. Implement BCA/CJIS Virtual Server requirements as outlined in the BCA/CJIS Policy, Section 5.10.3.2.

Logging Systems:

Purpose of Logging Systems: The purpose of logging systems is to advise the members of the advantage of a logging system to review and investigate incidents.

Optional Recommendations for Logging Systems:

1. Recommend the purchase of a logging system to record the logins, logouts, Windows events, and firewall events that occur on a member network.

2. Recommend the setting of the retention of the logs for 365 days to coincide with PCI and BCA requirements.

Virus/Malware Protection:

Purpose of Virus/Malware Protection: The purpose of virus/malware protection is to protect against unauthorized access and to protect LOGIS and LOGIS member's data. For the purpose of this section the term virus/malware is referred as malware protection.

Policy: Up-to-date malware protection, which includes protection from viruses, spyware, and other malicious software, is a requirement on all systems running operating system types commonly affected by malware. Malware on a member environment can affect all organizations. New malware is released daily, and to ensure the greatest protection antivirus servers must be set to download and distribute new definition files daily.

Common sense precautions should be taken. Users shall practice caution when visiting websites, downloading files and opening email attachments. Also, users shall not change their system's configuration or take other steps to defeat virus protection devices or systems. All systems that are part of the LOGIS WAN require up-to-date malware protection software.

Requirements for Malware Protection:

- Must run the most current version
- Definition files must be updated at least once a day

Optional recommendations for Malware Protection:

Additional protections against malware, such as:

- Host and/or network-based Intrusion Protection Systems.

Handheld Device Security:

Purpose of Handheld Device Security: The purpose of this section is to protect data residing on mobile phones and other handheld devices, which are becoming more common but have a far greater risk of being lost or stolen than traditional mobile computers. Handheld devices such as mobile phones or PDAs utilizing non-web mail viewing typically store the synced mail on the device itself, making the data more vulnerable.

Optional Recommendation for Handheld Device Security:

Handheld devices which utilize non-web mail or otherwise store non-public organization data should use additional device security features such as:

1. Screen locks requiring PINs or other measures for access to the device or data
2. Disallowing email attachments
3. Limiting email retention on the device
4. Having remote wipe capability if the device is lost or stolen along with defining this procedure appropriately in the organization's end user policies.
5. Implement Mobile Device Management (MDM) solution.

Internet:

Purpose of Internet: Access to the Internet through the LOGIS Wide Area Network (WAN) is a shared resource that most members utilize as a tool and is to be used for matters directly related to the business activities of that member and as a means to further the mission of providing services that are efficient, accurate, timely and complete.

In order to provide excellent services, software may monitor and limit internet activity in order to ensure the most efficient use of our valuable resources.

No expectation of privacy: Users should have no expectation of privacy as all files and documents, including personal messages and internet logs which are located on any member systems are subject to public open records requests.

Requirements for Internet: All users are responsible for adhering to professional standards when browsing the internet. Failure to adhere puts LOGIS and our members at risk for legal or financial liabilities, potential embarrassment and other consequences.

Optional Recommendations for Internet: LOGIS members should limit or prohibit inappropriate non-business access to the internet. Inappropriate non-business use includes, but is not limited to: bandwidth intensive video or movies, games, jokes, instant messaging, content of an offensive or pornographic nature, copyrighted material, and large data files not directly related to business. These types of files can be large and affect the network or computers performance or carry viruses.

Members should utilize a web-filtering product to monitor and filter internet web site access.

Electronic Mail (email):

Purpose of email: The email system is a tool to be used for matters directly related to the business activities of our members and as a means to further the mission by providing services that are efficient, accurate, timely and complete.

Public Nature of email: Email is a public record like any other public document. Email may be searched for evidence in any legal proceeding. By using the email system, the employee consents that in the event of suspicious activity their email system may be searched for evidence gathering purposes.

Policy: Employees are responsible for adhering to business standards when email is created, sent, forwarded or saved. Failure to adhere puts the organization and the individual at risk for legal or financial liabilities, potential embarrassment and other consequences.

This policy also applies to all contractors, consultants, volunteers, agents or any other persons who have gained or are given access to the email system.

Requirements for email:

1. Email is to be processed through antivirus/malware filtering software before being delivered to the members.
2. Emails with common attachments known to carry viruses/malware, e.g. .exe, must be eliminated from the email.
3. Outbound SMTP email must be eliminated from all non-email servers.
4. Email servers must be tested and verified that open relay is shut off on the server.
5. Email being sent cannot violate any Federal or State laws.
6. Web access to members email systems must utilize Digital Certificates using TLSv1.2 or greater for encryption.

Optional Recommendations for email:

1. Email should be filtered through an email filtering product to help eliminate SPAM email
2. Web access to members email systems should utilize Digital Certificates, using TLSv1.2 or greater, from a vendor that is a Trusted Certificate Authority.
3. Add DNS TXT SPF (Sender Policy Framework) records to limit forged spam effects.
4. Implementation of Domain based Message Authentication, Reporting and Conformance (DMARC).
5. Where possible, MFA for email web access should be utilized.
6. Internet email web access servers installed at the Member site should be installed in a DMZ in order to help protect the internal network environment.

Direct Inbound Internet Access:

Policy: Direct inbound access from the internet should normally be limited to just services on systems within the DMZ zone. The DMZ allows port 80, 443, and ftp/sftp to requested web sites unless otherwise approved. Approved connections should be restricted to only allow incoming traffic to specific ports on specific systems.

In the event where direct inbound access from the internet is needed to a system on another part of the member's network, any needed exceptions should be agreed upon between the member's IT management and LOGIS's Director of Infrastructure & Shared Services. These incoming connections should normally only be accepted from a very limited IP address range, with the exception of incoming email and web-based email access, unless otherwise approved. Ports 443 for web-based email and 25 for incoming email are allowed to the internal network.

VPN access is the only allowed less-restricted direct access from the internet.

Network Firewall and Infrastructure Segmentation:

Purpose of Infrastructure Segmentation and Firewall: To ensure proper security segmentation on the member networks to meet requirements of the PCI, CJIS, and LOGIS applications along with securing data in transmission to the LOGIS applications.

Policy: Member network segments that have direct internet or external organization access are required to install and maintain an industry standard firewall on their network to serve as a border device that is capable of stateful inspection. This firewall must segment the member network from the external access.

Optional Recommendations for Network Firewall and Infrastructure Segmentation:

1. Members should protect their network environment by installing and maintaining or utilizing an Intrusion Prevention System (IPS). These systems further secure the member networks by preventing network hacking and malware along with notifying members of suspicious activity.
2. Members should review their network environment and where logically possible segment departments, servers, applications into different network segments and filter traffic between these segments with access lists, firewalls, IPS devices.

Network Device Security:

Purpose of Network Device Security: The purpose of networking device security is to secure devices such as firewalls, routers, and switches against reconfiguration or other attacks.

Policy: Critical security patches for firewalls must be installed as soon as possible from the issued date.

Optional recommendations for Networking Device Security: Critical security patches for networking devices (excluding firewalls) should be installed within three months of release. Upgrade network equipment operating

system and firmware versions before they have reached end-of-life and replace network equipment before they have reached security patch end-of-life.

Remote Network Access:

Policy: Access to the LOGIS applications or network across an internet or public network requires an approved VPN to the LOGIS Wide Area Network (WAN). Remote access to the LOGIS or member network via VPN will be allowed only to employees or contractors authorized by the member's executive management. Approval and the specification of what resources will be available for access will need to be supplied before proceeding with the setup of any new VPN access.

VPN access is for the approved employees or contractors only and does not extend to other staff, family members, or other acquaintances.

In the event of a potential compromise of the VPN access, LOGIS will shut down the compromised VPN access until the situation is remedied.

The following sections outline two of the approved forms of VPN.

Network Access – LAN to LAN VPN

Policy: LOGIS will configure access to the LOGIS network via LAN to LAN VPN based on a minimum standard of AES 256 SHA2 encryption. Member network IP address ranges cannot conflict with existing routes and network addresses. If so, the member network must be NATed to a LOGIS assigned range through the tunnel.

Network Access – Client VPN

Supported Methods: LOGIS offers Cisco AnyConnect for unsupervised remote VPN network access. Any other unsupervised remote VPN methods should be agreed upon between the member's IT management and LOGIS's Director of Infrastructure & Shared Services.

Data Practices: Users should follow proper data practices protocols as directed by the Minnesota State Statutes. Storing of business-related information on a personal home or other remote computer creates an extension of the member's network, thus anything stored on that computer, might be subject to open records requests.

VPN access must be configured to use 128-bit or greater symmetric key data encryption.

All computers connected to the LOGIS WAN via VPN must also utilize personal firewall hardware and/or software.

VPN users are subject to all of the rules and regulations set forth in this policy for network use and any other related policies that apply.

Due to FBI and BCA security policies, MFA is recommended for mobile access to BCA data. Unique per-officer IP addresses are used by LOGIS to configure the VPNs to allow better audit of user access.

Cisco VPN: Every member will be issued one or more unique VPN authentication groups based on the function and security needs. The VPN group is assigned an IP range which is used to limit access to just the appropriate network locations, with the exception of Police groups using per-officer IP addresses. Example: a member could have the following groups:

City Hall Group
Police Group

IT Group

NetMotion VPN: Members that utilize NetMotion should have the software configured to issue a unique identifier that gets assigned along with its own unique IP in an IP range. Each member will have one or more unique NetMotion IP ranges that are used to limit access to just the appropriate network locations.

Requirements for Remote Access:

1. Client based VPN's must utilize MFA to establish remote access in order to secure the credentials and further limit access from outside malicious users.
   Enforcement effective December 31, 2024

Optional Recommendation for Remote Access:

1. Client based VPNs should be configured in a full tunnel mode where all traffic is sent over the VPN. This sends member internet traffic through existing security controls and filters to detect or block malware activity that can be missed in a split-tunnel configuration. The use of a "split-exclude" list should be used if required for local resources (such as in-car video systems).
2. Client based VPNs with full network access should only be permitted from member owned or controlled equipment wherever possible.
3. Client based VPNs from non-member owned or controlled equipment (such as contractors) should be restricted to the minimum inside hosts or networks required.

Wireless Networking:

Purpose of Wireless Networking: Wireless networking is in use at our member organizations. Wireless network signals may extend beyond the walls of the physically secure area and present a unique risk. To address the security issues, LOGIS has developed the following policy for wireless networking:

Policy: The following are requirements for all wireless access points:

For access points that do not block all direct access to the member's network

1. All access points must be defined on a form of DMZ or use access lists that only allow access to limited resources on the member's network.
2. Access must be limited to devices authorized by the IT staff.
3. 128 bit or greater encryption must be used, using an approved algorithm considered secure.

Additional requirements for 802.11 access points:

1. The SSID must be changed from the default SSID.
2. WPA with AES-CCMP or WPA2 encryption must be used on all 802.11 devices due to weakness in WEP and WPA with TKIP.

Public / Guest wireless network access must not be able to access the member's regular network without the use of a VPN.

Optional Recommendations for 802.11 Wireless Access:

1. An approved VPN and/or WPA2-Enterprise (example: Active Directory Wi-Fi authentication) security should be used for access to member networks from wireless access points rather than relying solely on WPA2 with a shared password.
2. WPA2-Enterprise (e.g. user's password) is recommended rather than WPA-PSK (shared password), as Windows 7 displays the password where it could be viewed and used by unauthorized persons.
3. WPA2-Enterprise using PEAP/MSCHAPv2 authentication should be set to specify the CA certificate used, the server certificate CN name, and prohibit popups that bypass authentication security warnings.
4. Hide Wi-Fi pre-shared keys (passwords) from users if they are allowed local administrator rights, by setting registry permissions on the Software Class AppIDs {86F8…} and {C100…} in group policy.

5. Public wireless should be public DNS servers and not member's local AD/DNS servers.
6. Implement rouge wireless access point detection and maintain current list of authorized networks and devices.

Multifunction Device and Network Printers Security:

Purpose of Multifunction Device and Network Printers Security: There are general principles involved in securing network-attached multifunction devices (MFDs), digital senders, and network printers. MFDs provide printing, copying, faxing, and scanning services from a single network-accessible device. Similar to computers, MFDs and many network printers include an operating system, usually embedded, and network connectivity. These devices can use network protocols, such as File Transfer Protocol (FTP), telnet, Hyper Text Transport Protocol Secure (HTTPS), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). MFDs may also have a connection to an analog line for fax functionality. As more functionality has been added to these devices, the security vulnerabilities and risk to organizational data are becoming similar to those of other network devices.

Optional Recommendations for Multifunction Device and Network Printers Security:

1. Update the firmware.
2. Disable unneeded services, protocols, and features.
3. Restrict access to the device based on required protocols and IP address ranges.
4. Allow setting and changing of the authentication information (e.g., passwords and community strings) for all management services.
5. Prevent unauthorized physical access to the hard drive using either a locking mechanism or other physical access control measure.
6. Implement authenticated access to management controls, allowing access to authorized administrators based on privilege assignments.
7. Enable and configure audit logging (Syslog capability preferred).
8. Disable FTP and SSH unless using to upgrade firmware.
9. Disable DHCP and ensure device has a dedicated/static IP.
10. Disable Bootstrap Protocol (BOOTP).
11. Use SNMPv3 for system notifications such as paper jams and low toner.
12. Replace all default passwords and community strings with complex passwords
13. Place all MFD's and Network printers on a dedicated network segment or VLAN with a discretionary access list limited to the IP Addresses of the system administrators and print spoolers.
14. Disable wireless printing features, such as Apple AirPrint and HP Wi-Fi Direct, which allow mobile device users the ability to print directly to a MFD or printer. Wireless direct printing bypasses the print spooler, which prevents authentication of the user and logging of print jobs.
15. Secure access to the device's configuration and management functions.
16. Secure print, copy, scan, and fax jobs against unauthorized access and delete when no longer needed.

Programs and Software:

Copyright Laws: Most computer software and programs, applications and templates are copyrighted, and it is illegal to make copies.

Policy: Employees or contractors may under no circumstances make any copies of member's or our privately owned or licensed software. All employees or contractors are required to abide by federal copyright laws and to abide by all such licensing agreements. If there is any question about the legality and appropriate use of the software, it should be directed to the member's IT staff.

Security Tools:

Policy: Security auditing tools must only be used by individuals authorized by their management. Scanning/sniffing of the LOGIS internal network or other member organizations without prior LOGIS/member management approval is not allowed. Members planning to perform network penetration scans that extend past their organization and/or utilize the LOGIS internet bandwidth must notify LOGIS 7 days in advance.

Security Incident Reporting:

Policy: The member's IT policy must require staff to immediately report to their IT department any suspected computer or network security incident. This can include loss of hardware or software, compromise of systems, or other suspected security events. Member's IT staff will notify LOGIS immediately if applicable. Compromise of the workstations include but are not limited to viruses, spyware, etc. Other types of security events include accounts suspected to be compromised, or social engineering such as someone demanding a password.

It is recommended that members use the NIST standard in incident documentation and reporting in order to define a reportable incident.

https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Security Incident Response:

Members are responsible for establishing, documenting, and distributing their own security incident response and escalation procedures to ensure timely and effective handling of suspected security incidents.

Members are responsible for reporting any known or suspected breach of LOGIS security to LOGIS management.

Security Training:

Policy: Annual security awareness training is required to make end users aware of security policy as well as best practices in preventing other threats such as social engineering. Samples of topics relevant to member end users include: Member IT policies, unsolicited UPS/bank email attachments, calling IT immediately if users receive a real or fake malware alert, not browsing police/non-public data (with news headlines), thumb drive security, social engineering / trick calls or emails, creating good passwords, malicious video web browser plugin requests, security incident reporting, etc.

Section 5 – Separation of Employees and Vendors

Purpose:

The purpose of this section is to establish procedures that will occur when an employee or vendor is separated for any reason, whether voluntarily or involuntarily, at a member organization. This section is required to maintain security and confidentiality of the member's data and systems.

Policy:

The member's IT staff is required to notify LOGIS of separated employees and vendors that access LOGIS applications and systems.

LOGIS, upon receiving notification, will immediately disable access on the user account from the respective applications and systems.

Due to the complexity of the applications and systems, please supply LOGIS with as much notice as possible.

The member's IT staff will be required to audit their LOGIS account user list annually to validate accounts and ensure privileges are appropriate.

Section 6 – Vendor Remote Access

Purpose:

The purpose of this section is to establish procedures that govern vendor remote access into the network and/or systems. This is required to maintain security and confidentiality of the data and systems. The three approved methods of vendor remote access are: VPN, and LOGIS collaboration and conference software such as Webex, GoToMeeting, etc. The member's IT manager or LOGIS's Director of Infrastructure & Shared Services may also approve additional web-based remote-control products they have validated for security, provided the end-user can interactively monitor and control the session.

Requirements for Vendor Remote Access:

1. Vendor remote access must be disabled until access is required.
2. All modems must remain powered off until required for remote access.
3. The member is responsible for validating the vendor's identity before enabling the session.
4. The person enabling access is also responsible for disabling access immediately after the vendor is completed.
5. Initial setup of remote access is not allowed without prior approval of IT management.
6. Vendor user accounts and VPN configurations must be restricted to the minimal access required.
7. Vendors not vetted by the BCA are not allowed unsupervised remote access to the police segments reserved for the BCA.
8. All security requirements must be followed as defined under this document.

Optional Recommendations for Vendor Remote Access:

1. The vendor should be set up with local accounts on the machines that are being accessed.
2. The vendor should define the changes that will be performed and these changes should be recorded.
3. Member is responsible for monitoring remote sessions and work performed by vendor.
4. Remote access sessions should be used in conjunction with approved member staff.
5. MFA should be used for vendor remote VPN access into member networks.

Section 7 – Audit

Purpose:

The purpose of this section is to provide the authority for LOGIS to work in conjunction with the organizations IT staff to conduct targeted audits of their systems and network in an effort to maintain an adequate level of security.

LOGIS may conduct an audit of member networks and systems at any point to ensure compliancy with this policy. LOGIS will perform a full security audit of five randomly selected members per year.

This policy strives to create an environment within LOGIS and our members that maintain system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data.

Audits are conducted to:

- Ensure integrity, confidentiality and availability of information and resources.
- Investigate possible security incidents and to ensure conformance to LOGIS security policies.
- Monitor users when directed by management.
- Monitor system activity, this would include telecommunications traffic, WAN bandwidth, and server performance. Example: A virus would cause additional traffic.

Policy:

This policy covers all computers, communication devices, and media owned or operated by the members. This policy also covers any devices used for official business which may not be owned or operated by the member organization.

When requested, or for the purpose of performing an audit, any access needed will be provided to member's IT staff and/or LOGIS staff and/or an independent organization contracted by the member to perform such an audit.

This access may include:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on LOGIS equipment, storage media or premises.
- Access to work areas (labs, offices, cubicles, home sites, storage areas, etc.).
- Access to interactively monitor and log traffic on LOGIS or member networks.
- Access to email or any other electronic communication.

This policy is not intended to supersede any LOGIS member agreements or existing state or federal laws.

Audit Results:

Audit results will be supplied to the member's IT staff. The member will resolve and correct any security issues upon discovery in a timely manner and all audit trail files and/or results must be protected to prevent unauthorized changes or destruction.

Section 8 – New LOGIS Membership

Policy:

New members will be provided a copy of the LOGIS Members Security Policy. The new member will be required to comply to the policy. To allow the new member to make adequate changes to their environment a grace period of six months can be granted for the sections of Password Management, General Management, and Vendor Remote Access. A year grace period can be granted for the section of Physical Security.