**Gardner Valley School**
**Criminal History Record Information (CHRI)**
**Proper Access, Use, and Dissemination Procedures**

## Purpose

The intent of the following policies is to ensure the protection of the Criminal Justice Information (CJI) and its subset of Criminal History Record Information (CHRI) until such time as the information is purged or destroyed in accordance with this policy.

The following policies were developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy, meeting the minimum standards, but modified to meet the needs of GVS.

## Scope

The scope of this policy applies to any electronic or physical media containing CJI while being stored, accessed or physically moved from a secure location from Gardner Valley School (GVS). In addition, this policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media containing CJI.

## Criminal Justice Information (CJI) and Criminal History Record Information (CHRI)

CJI is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. Most commonly, this includes fingerprint and background check information for employees.

CHRI, is a subset of CJI and for the purposes of this document is considered interchangeable. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI.

## Proper Access, Use, and Dissemination of CHRI

Information obtained from the Interstate Identification Index (III) is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing noncriminal justice administrative functions on behalf of the authorized recipient and the outsourcing of said functions has been approved by appropriate CJIS Systems Agency (CSA) or State Identification Bureau (SIB) officials with applicable agreements in place.

## Roles and Responsibilities:

**Local Agency Security Officer (LASO)**
Each LASO shall:

1. Identify who within GVS is using the approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure that approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the appropriate persons are promptly informed of security incidents.
6. Serve as the security point of contact to the FBI CJIS Division ISO.
7. Document technical compliance with this Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to authorized personnel throughout the GVS's user community.
8. Document and provide assistance for implementing the security-related controls for GVS and its users.
9. The LASO has been identified as the point of contact on security-related issues for GVS and shall ensue the incident response reporting procedures at the local level.

**Information Technology Support**

In coordination with the LASO, all vetted IT support staff will protect CJI from compromise at GVS by performing the following:

1. Protect information subject to confidentiality concerns-in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, and internet connections as authorized by GVS. For agencies who submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.
2. Be knowledgeable of required GVS technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit and at the end of life.
3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.
4. Properly protect GVS's CJIS system (s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).
    a. Install and update antivirus on computers, laptops, MDTs, servers, etc.
    b. Scan any outside non-agency owned CDs, DVDs, thumb drives, etc., for viruses, if GVS allows the use of personally owned devices.
5. Data backup and storage-centralized or decentralize approach.

a. Perform data backups and take appropriate measures to protect all stored CJI.
b. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from physically secured location.
c. Ensure any media released from GVS is properly sanitized/ destroyed. (See Media Sanitization and Destruction Policy)

6. Timely application of system patches-part of configuration management.
   a. The agency shall identify application, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
7. Access control measures
   a. Address least privilege and separation of duties.
   b. Enable event logging of:
      - Successful and unsuccessful system log-on attempts.
      - Successful and unsuccessful attempts to access, create, write, delete or change Permission on a user account, file, directory or other system resource.
      - Successful and unsuccessful attempts to change account passwords.
      - Successful and unsuccessful actions by privileged accounts.
      - Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
   c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
8. Account Management in coordination with LASO
   a. Agencies shall ensure that all user IDs belong to currently authorized users.
   b. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.
   c. Authenticate verified users as uniquely identified.
   d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
   e. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.
   f. Passwords
      - Be a minimum length of eight (8) characters on all systems
      - Not be a dictionary word or proper name.
      - Not be the same as the User ID.
      - Expire within a maximum of 90 calendar days.
      - Not be identical to the previous ten (10) passwords.
      - Not be transmitted in the clear or plaintext outside the secure location.
      - Not be displayed when entered.
      - Ensure password are only reset for authorized user.
9. Network infrastructure protection measures.
   a. Take action to protect CJI-related data from unauthorized public access.
   b. Control access, monitor, enabling and updating configurations of boundary protection firewalls.

c. Enable and update personal firewall on mobile devices as needed.
d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and *advanced authentication when leaving a physically secure location. No confidential
e. data should be transmitted in clear test. *Note: a police vehicle shall be considered a physically secure location.
f. Ensure any electronic media that is removed from a physically secured location is encrypted in transit by a person or network.
g. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.
h. Make sure law enforcement networks with CJI shall be on their own network accessible by authorized personnel who have been vetted by GVS. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.

10. Communicate and keep GVS informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to GVS.

**Media Storage and Access**

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. For purposes of this policy, "electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card that contain CJI; "physical media" includes printed documents and imagery that contain CJI.

To protect CJI, GVS personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed or digital media from the CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures.
5. Not use personally owned information system to access, process, store, or transmit CJI unless GVS has established and documented the specific terms and conditions for personally owned information system usage.
6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
7. Store all hardcopy CJI printouts maintained by GVS in a secure area accessible to only those employees whose job function requires them to handle such documents.
8. Safeguard all CJI by GVS against possible misuse by complying with this policy.

9. Take appropriate action when in possession of CJI while not in a secure area:
    a. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
    b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in physically secure location, the data shall be immediately protected using encryption.
        - When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.
        - When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
10. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.
11. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI. (See Physical Protection Policy)

**Physically Secure Location:**

A physically secure location is a facility or an area, a room or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in GVS shall be defined with a sign at the entrance.

**Visitors Access:**

A visitor is defined as a person who visits GVS facility on a temporary basis who is not employed by GVS and has no unescorted access to the physically secure location within GVS where CJI and associated information systems are located.

Visitors shall:

1. Check in before entering a physically secure location by:
    a. Provide a form of identification used to authenticate visitor.
    b. If GVS issues visitor badges, the visitor badge shall be worn on approved visitor's outer clothing and collected by the agency at the end of the visit.
2. Be accompanied by a GVS escort at all times to include delivery or service personnel. An escort is defined as authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically

secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

3. Show GVS personnel a valid form of photo identification.
4. Follow GVS policy for authorized unescorted access.
    a. Private contractors/vendors who requires frequent unescorted access to restricted area (s) will be required to establish a Security Addendum between GVS and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.
5. Not be allowed to view screen information mitigating shoulder surfing.
6. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.
7. Not be allowed to sponsor another visitor.
8. Not enter into a secure area with electronic devices unless approved by GVS Local Area Security Office (LASO) to include cameras and mobile devices. Photographs are not allowed without permission of GVS assigned personnel.
9. All requests by groups for tours of GVS facility will be referred to the proper point of contact for scheduling and monitoring.

**Authorized Physical Access:**

Only authorized personnel will have access to physically secure non-public locations. GVS will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All personnel with CJI physical and logical access must:

1. Meet the minimum personnel screening requirements prior to CJI access.
    a. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI.
    b. Complete security awareness training.
    a. All authorized GVS personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.
    b. Security awareness training will cover the CJIS Security Policy at a minimum.
2. Be aware of who is in their secure area before accessing confidential data.
    a. Take appropriate action to protect all confidential data.
    b. Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.
3. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.
    a. Report loss of issued keys, proximity cards, etc. to authorized agency personnel.

    b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call GVS point of contact to have authorized credentials like a proximity card deactivated and/or door locks possibly rekeyed.
    c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. (See Disciplinary Policy).
4. Properly protect from viruses, worms, Trojan horses, and other malicious code.
5. Do not use personally owned devices for CJI access.
6. Use of electronic media is allowed only by authorized GVS personnel.
7. Encrypt emails when electronic mail is allowed to transmit CJI-related data as such in the case of Information Exchange Agreements.
    a. If CJI is transmitted by email, the email must be encrypted (FIPS 140-2) end-to-end and email recipient must be authorized to receive and view CJI.
8. Report any physical security incidents to GVS's LASO to include facility access violations, loss of CJI, loss of laptops, cell phones, thumb drives, CDS/DVDs and printouts containing CJI.
9. Properly release hard copy printouts of CJI only to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printout when no longer needed. Information should be shared on a "need to know" basis.
10. Ensure data centers with CJI are physically and logically secure.
11. Keep appropriate GVS security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.
12. Not use food or drink around information technology equipment.
13. Know which door to use for proper entry and exit of GVS and only use marked alarmed fire exits in emergency situations.
14. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries.

**Media Transport**

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use.

Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

GVS personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

GVS personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CJI.
3. Following the least privilege and role based rules for allowing access. Limit access to CJI to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
    a. Storing CJI in a locked briefcase or lockbox.
    b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
    c. For hard copy printouts or CJI documents:
        - Package hard copy printouts in such a way as to not have any CJI information viewable.
        - That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by methods (s) that provide for complete shipment tracking and history, and signature confirmation of delivery. (Agency Discretion)

5. Not taking CJI home or when traveling unless authorized by GVS LASO. When disposing confidential documents, use a cross-cut shredder.

**Breach Notification and Incident Reporting**

GVS shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. GVS personnel shall notify his/her supervisor or LASO, and an incident-report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident.
2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI records.
3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.

4. The CSA ISO will:
    a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency,

and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
    b. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
    c. Act as a single point of contract for their jurisdictional area for requesting incident response assistance.
5. If CHRI is lost, stolen, misused, or there is a breach of information, the following people will be notified:

CJIS Information Security Officer-Emily Philip @303-239-4237
Email: emily.philip@state.co.us

**Penalties**
Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or employment termination.

**Retention Policy**

**Retention of CHRI**
Federal law prohibits the repurposing or dissemination of CHRI beyond its initial requested purpose. Once an individual's CHRI is received, it will be securely retained in internal agency documents for the following purposes ***only***:

- Historical reference and/or comparison with future CHRI requests
- Dispute of the accuracy of the record
- Evidence for any subsequent proceedings based on information contained in the CHRI. CHRI will be kept for the above purposes in:
    - hard copy form in personnel files located in the locked filing cabinet located in the locked filing room

**Retention Guidelines**
- All CHRI is stored in a secure location.
- CHRI is never left unattended, (physically on a desk or electronically on a computer screen in the SDDS).
- Once the document is printed, it is immediately placed in a locked filing cabinet. During "afterhours", the entrance to the office is also locked.
- CHRI is only physically transported from the printer to the locked filing cabinet.
- Visitor Controls-Visitors are not allowed to enter the office unescorted and without a badge.
- GVS ensures that the processing of applicant requests and/or CHRI responses is only accessible by those authorized to view CHRI.
- GVS stores hard copy results (not electronic copies) of CHRI in a locked filing cabinet located in the HR Office which is also locked.

**Duration**
Employee criminal history record information (CHRI) shall be confidentially maintained in the employee's personnel file and retained for 10 years after retirement or separation according to schedule 15 of the Colorado School District Records Management Manual.

**Destruction**
CJI/CHRI will be destroyed when its purpose has been fulfilled and regulatory guidelines have been satisfied.

**Media Sanitization and Destruction Policy**

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs and other similar items used to process, store and/or transmit CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by GVS.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

1. Shredded using GVS issued cross-cut shredders

2. Placed in locked shredding bins for private contractor to come on-site and cross-cut shred, witnessed by GVS personnel throughout the entire process

3. Incineration using GVS incinerators or witnessed by GVS personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one of GVS methods:

1. **Overwriting (at least 3 times)-**an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

2. **Degaussing-**a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g. those used to hand a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

3. **Destruction-**a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit CJI and/or sensitive and classified information shall not be released from GVS's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

**Discipline Policy for Misuse**

Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statues. All files are subject for search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction (s). Complaints alleging misuse of GVS's computing and network resources and MI/FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

**Examples of Misuse with access to CJI**

1. Using someone else's login.
2. Leaving computer logged in with your login credentials unlocked, allowing anyone to access GVS systems and/or CJIS systems and data in your name.
3. Allowing unauthorized person to access CJIS at any time for any reason. Note: Unauthorized use of the CJIS systems is prohibited and may be subject to criminal and /or civil penalties.
4. Allowing remote access of GVS issued computer equipment to CJIS systems or data without prior authorization by GVS.
5. Obtaining a computer account that you are not authorized to use.
6. Obtaining a password for a computer account of another account owner.
7. Using GVS's network to gain unauthorized access to CJI.
8. Knowingly performing an act which will interfere with the normal operation of CJIS systems.
9. Knowingly propagating a computer virus, Trojan horse, worm, and malware to circumvent data protection or compromising existing security holes to CJIS systems.
10. Masking the identity of an account or machine.
11. Posting materials publicly that violate existing laws.
12. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner.
13. Unauthorized possession of, loss of, or damage to GVS's technology equipment with access to CJI through unreasonable carelessness or maliciousness.
14. Maintaining CJI or duplicate copies of official GVS files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.
15. Using GVS's technology resources and/or CJIS systems for personal or financial gain.
16. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.

The above listing is not all-inclusive and any suspected technology resource or CJIS system or CJI misuse will be handled by GVS on a case by case basis. Activities will not be considered misuse when authorized by appropriate GVS officials for security or performance testing.

**Misuse Notification**

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, GVS shall: (i) establish an operational incident handling capability for all information systems with access to CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

All GVS personnel are responsible to report misuse of GVS technology resources to appropriate GVS officials.

Local contact-LASO: [W.Denise Johnson] Phone- [719-746-2446]

**Incident Response Policy**

All individuals with direct or indirect access to CHRI shall be trained on how to handle an information security incident, and such training is to be included within the agency's Security Awareness Training. A procedure shall be in place to track and document information security incidents, whether physical or digital, on an ongoing basis. When an incident has been determined a breach involving CHRI, the agency will report the security breach to the MSP ISO by use of the "Information Security Officer (ISO) Computer Security Incident Response Capability Reporting" form (CJIS-016).

a. In the event of an Incident, the following people should be notified immediately: Executive Director- Jody Medina (Head of School) who will notify the LASO. LASO-[W. Denise Johnson] (School Secretary)
b. Handling Capabilities implemented by the agency:

| Capabilities shall be handled according to the following description: | Physical – Hard Copy CHRI | Digital – Digitally Accessed/Saved CHRI |
|---|---|---|
| 1. Preparation | The CHRI container will be locked at all times in the HR office which will be locked when office staff is not present.<br>Video system in use-24/7 | Firewalls, virus protection, and malware/spyware protection will be maintained. |
| 2. Detection | Physical intrusions to the building will be monitored by means of: The building is monitored by the school's | Electronic intrusions will be monitored by the virus and malware/spyware detection. |

| | | |
|---|---|---|
| | alarm system and cameras. The doors are checked and locked every night by the maintenance staff. | |
| 3. Analysis | The LASO will work with police authorities to determine how the incident occurred and what data were affected. | IT department will determine what systems or data were compromised and affected. |
| 4. Containment | The LASO will lock uncompromised CHRI in a secure container or transport CHRI to secure area. | The IT department will stop the spread of any intrusion and prevent further damage. |
| 5. Eradication | The LASO will work with law enforcement Arapahoe County Sheriff's Office to remove any threats that compromise CHRI data. | The IT department will remove the intrusion before restoring the system. All steps necessary to prevent recurrence will be taken before restoring the system. |
| 6. Recovery | The law enforcement agency Arapahoe County Sheriff's Office in charge will handle and oversee recovery of stolen CHRI media. The LASO may contact MSP for assistant in re-fingerprinting if necessary. | The IT department will restore the agency information system and media to a safe environment. |

c. LASO shall collect information using the Security Incident Response Form. Provided GVS decide to take legal action, whether criminal or civil, Arapahoe County Sheriff's Office will be notified or the school attorney will be contacted in a civil matter.
d. Reporting - an "Information Security Officer (ISO) Computer Security Incident Response Capability Reporting," form has been established, and is the required method of reporting security incidents to the LASO.
e. The ISO-Security Incident Reporting form will be used for the reporting of security incidents. GVS will retain completed forms on an ongoing basis in order to meet policy requirement for tracking.

**Adopted:** Oct 19, 2022