<u>FILE:</u> **GBEB_F**

MOUNTAIN BOCES

ACCESS, STORAGE, AND SECURITY OF SENSITIVE STAFF RECORDS

I. Purpose

The purpose of the below policies is to protect the privacy of sensitive and classified employee information.

II. Staff Fingerprints

The Mtn BOCES requires some staff members to provide fingerprints when they accept employment with the Mtn BOCES. Board Policy GBEB. The Mtn BOCES keeps records of staff fingerprints, which may be requested by a local, state, or federal government agency or private individual. The Mtn BOCES shall keep record of each request for staff fingerprints for five (5) years, including:

(1) the name and address of the person or agency to whom the Mtn BOCES disclosed the fingerprints;
(2) the date the person or agency requested the fingerprints;
(3) the nature of the agency or person's request;
(4) the purpose for which the Mtn BOCES disclosed the fingerprints.

III. Security of Criminal History Record Information

The Mtn BOCES conducts fingerprint-based criminal history record checks of its employees. Board Policy GBEB. As such, it keeps records of employees' criminal history information ("Criminal History Record Information") or ("CHRI"). The purpose of this policy is to provide transparency and guidance with respect to the storage and disposal of such information, as well as to outline procedures to report misuse of CHRI, document breaches, and security violations.

A. Handling, Storage, and Disposal

Storage: The Mtn BOCES shall securely store digital and physical media containing CHRI within physically secure locations or controlled areas. The Mtn BOCES shall restrict access to digital and physical media to authorized individuals.

Handling: When transporting media containing CHRI, the Mtn BOCES shall protect and control such media, and shall restrict the transportation of such media to authorized personnel.

Disposal: The Mtn BOCES shall dispose of media containing CHRI in the following manner:

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

1) shredding using Mtn BOCES-issued shredders.

2) placed in locked shredding bins for a third party vendor to come on-site and shred, witnessed by *Mtn* BOCES personnel throughout the entire process.

3) incineration using Mtn BOCES incinerators or witnessed by *Mtn* BOCES 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 the Mtn BOCES 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 hang 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 CHRI and/or sensitive and classified information shall not be released from the Mtn BOCES's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Documentation: The Mtn BOCES shall maintain written documentation of the steps taken to sanitize or to destroy electronic media containing CHRI.

B. Misuse of Criminal History Record Information

The Mtn BOCES prohibits the use of CHRI for any unlawful purpose under state or Federal law ("misuse").

Procedure: If misuse of CHRI is reported to the Mtn BOCES or if, for any reason, the Mtn BOCES suspects that an employee or agent of the Mtn BOCES is misusing CHRI, that employee or agent's direct supervisor shall notify the human resources ("HR") department and the employee shall temporarily be restricted from accessing CHRI. The HR department shall investigate the alleged misuse of CHRI and shall make findings with respect to whether the employee or agent misused CHRI.

Sanctions: If the Mtn BOCES finds that an employee or agent of the Mtn BOCES has misused CHRI, it may result in loss of access to CHRI, loss of employment, and/or criminal prosecution. Misuse of CHRI shall constitute just cause to terminate any employee's employment with the Mtn BOCES.

Reporting: The Mtn BOCES shall report all findings of misuse of CHRI to the Colorado Bureau of Investigations.

C. Procedures to Report and Document Breaches of Information and Security Violations

Implementation: The Mtn BOCES shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. When possible, the Mtn BOCES shall employ automated mechanisms to support the incident handling process.

The Mtn BOCES shall incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

Reporting: The Mtn BOCES shall track, document, and report incidents to the Colorado Bureau of Investigation.

D. Authentication

All digitally stored CHRI shall be password-protected.

Password requirements: The Mtn BOCES shall require all passwords to contain nine characters, including at least four numbers, one capital letter, and one special character. The password shall not be a dictionary word or proper name. The password shall not be the same as the UserID. Passwords shall not be displayed when entered

Password reuse constraints: The password must not be identical to the user's previous ten (10) passwords.

Maximum expiration of password: Passwords shall expire after ninety days and must be reset before such time.

E. Encryption

The Mtn BOCES shall protect its digitally stored data containing CHRI using encryption. The cryptographic module used shall be FIPS 197 certified and shall use a symmetric cipher key strength of at least 256 bit strength.

(Adoption Date)