

EMPLOYMENT REQUIREMENTS AND RESTRICTIONS
CRIMINAL HISTORY AND CREDIT REPORTS

DBAA
ADMINISTRATIVE REGULATION

EMPLOYMENT REQUIREMENTS AND RESTRICTIONS
CRIMINAL HISTORY AND CREDIT REPORTS

DBAA
ADMINISTRATIVE REGULATION

- Any further information provided by the person concerning his or her criminal history record.
- The employee's conduct during his/her employment with the District, where applicable.
- Input from the employee's immediate supervisor, where applicable.

An employee may be placed on administrative leave with or without pay, as appropriate, while the District collects facts facts

{ &

EMPLOYMENT REQUIREMENTS AND RESTRICTIONS
CRIMINAL HISTORY AND CREDIT REPORTS

DBAA
ADMINISTRATIVE REGULATION

The following individuals must have passed the third-party county-by-county (long) background review before the approval process can proceed:

- Adult temporary hires not working directly with students
- Independent contractors not working directly with students
-

EMPLOYMENT REQUIREMENTS AND RESTRICTIONS
CRIMINAL HISTORY AND CREDIT REPORTS

DBAA
ADMINISTRATIVE REGULATION

Only authorized personnel will have access to the physically secure locations. The District will maintain and keep current a list of authorized personnel. The District will implement access controls and monitor physically secure areas to protect all transmission and display media of CHRI. Authorized personnel will take necessary steps to prevent physical, logistical, and electronic breaches.

Physical media such as printouts will be disposed of by one of the following methods:

- Shredding using District shredders;
- Placement in locked shredding bins for an authorized shredding contractor to come to District premises and shred, witnessed by District personnel throughout the entire process; or
- Incineration using District incinerators or by an authorized incineration contractor, witnessed by District personnel either at a District or contractor incineration site.

Electronic media such as hard drives, tape cartridges, CDs, printer ribbons, or printer and copier hard drives will be disposed of by one of the following methods:

- Overwriting at least three times. Overwriting uses a program to write binary code onto the location of the file needing sanitization.
- Degaussing. Degaussing magnetically erases data from magnetic media, using strong magnets or electric degaussers.
- Destruction. Destruction involves physically dismantling electronic media by methods such as crushing or disassembling, ensuring that the platters have been physically destroyed so that no data can be retrieved.

Information technology systems that have been used to process, store, or transmit CHRI will not be released from the District's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

ACCOUNT
MANAGEMENT

The District will manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The District will validate information system accounts at least annually and shall document the validation process.

All accounts will be reviewed at least annually by the POC or designee to ensure that access to and account privileges on systems that contain CHRI are commensurate with job functions, need-to-know, and employment status. The POC may also conduct periodic reviews.

EMPLOYMENT REQUIREMENTS AND RESTRICTIONS
CRIMINAL HISTORY AND CREDIT REPORTS

DBAA
ADMINISTRATIVE REGULATION

The District will authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store CHRI. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-District-controlled network (e.g., the Internet).

The District will employ automated mechanisms to facilitate the monitoring and control of remote access methods. The District will control all remote accesses through managed access control points. The District may permit remote access for privileged functions only for compelling operational needs, but will document the rationale for such access in the security plan for the information system.

Utilizing publicly accessible computers to access, process, store, or transmit CHRI is prohibited. Publicly accessible computers include, but are not limited to, hotel business center computers, con-

EMPLOYMENT REQUIREMENTS AND RESTRICTIONS

DBAA

CRIMINAL HISTORY AND CREDIT REPORTS

ADMINISTRATIVE REGULATION

action, up to and including loss of access privileges, termination, and/or civil or criminal prosecution.

Violation by a visitor of any requirements of this policy or the most recent CJIS Security Policy will result in suitable disciplinary action against the sponsoring employee, up to and including loss of access privileges, termination, and/or civil or criminal prosecution.

Credit History

The District shall obtain credit history information in accordance with the Fair Credit Reporting Act on a candidate for employment in the following positions: Superintendent; Chief Financial Officer; Executive Director of Finance; Director of Budget, Taxes and Investments; Director of Payroll and Benefits; and when a candidate's credit history is related to the position for which the person is being considered.