Background Check Policy

(1) In accordance with USHE Policy R847, which is incorporated herein by reference:
  (a) All applicants for employment must submit to a criminal background check as a condition of employment, except for temporary positions exempted by the President or the Vice President of Administrative Services; and
  (b) An employee shall submit to a background check when required by the President or the Vice President of Administrative Services when the President or Vice President find that reasonable cause exists.
(2) Before an applicant is denied employment or an employee is subject to an adverse employment action based on information obtained in a background check, the applicant or employee shall have an opportunity to respond in accordance with R847-4.10.
(3) Security shall establish and maintain a livescan machine which provides the means to submit digital criminal background information to the state for the purpose of obtaining criminal background information from both state and federal checks. The person whose background is being checked is required to sign an authorization form which allows the College to conduct a criminal background check.
(4) A Risk Assessment shall be made by the College's Vice President of Administrative Services in consultation with other persons making the employment and promotion decision as appropriate.
(5) Background Check Information Management.
  (a) Personnel Sanctions Policy. Background checks and results may only be used for authorized purposes, and those employees with account access are responsible for securing and protecting the information.
    (i) Employees misusing or failing to secure or protect the information are subject or discipline, possibly including loss of access privileges and termination of employment.
    (ii) All such incidents shall be reported to the College President.
    (iii) At a minimum, employees who violate this policy more than two times in a 12-month period have their privileges revoked for a period of not less than one year.
  (b) Security Awareness Training Policy. The HR Department shall provide training to each employee with account access and access to background check information upon hire, and yearly thereafter. The Security Department shall provide yearly training to employees authorized to submit background checks.
  (c) Physical Protection, Physical Security and Media Disposal Policy.

(i) Employee background check results will not be downloaded onto the College server or any College computer. Any physical copies of results must be secured and kept within an HR Officer's personal control, and, upon the relevant employment or promotion decision having been made, destroyed by shredding.

(ii) Student background check results shall be scanned and maintained electronically on an encrypted secure drive separate from the College server. The physical copies of the student background checks results shall be shredded immediately upon them being scanned. The secure drive shall be maintained in a locked location, with access limited to the person(s) designated to review those results by the Vice President of Administrative Services. No other persons shall have access. Student background check results shall be deleted from the secure drive in the third calendar year following them being scanned. Any physical copies of results must be secured and kept within the control of the designated person(s), and, upon the relevant admission decision having been made, destroyed by shredding.

(d) Personnel Security Policy. All persons who are authorized to conduct background checks or access background check information shall be employees of the college who have had a complete background check.

(e) Auditing and Accountability Policy. Dixie Tech reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy. For security and network maintenance purposes, authorized individuals within Dixie Tech may monitor equipment, systems and network traffic at any time. The HR and Security Departments shall conduct a yearly audit to assess compliance with legal requirements, and make a written assessment of deficiencies and possible improvements to College policies and procedures.

(f) Mobile Device Policy. No account access may be made on mobile devices (not including College laptops), and no background check information may be stored on such devices.

(g) Personally Owned Devices and Publicly Accessible Computers Policy. No account access may be made with an employee's personally owned device or on publicly available computers, and no background check information may be stored on such devices.

(h) Access and Identification Policy.

(i) Employees shall be assigned unique accounts, and employees may not share account information. Employees shall log out of the system immediately after obtaining the necessary information.

(ii) Access to background check information must be made through a secure connection.

(iii) The Vice President of Administrative Services must be notified if a user's information system usage or need-to-know changes.

(iv) The Vice President of Administrative Services shall:

(A) Disable all new accounts that have not been accessed within one month of creation. Accounts of individuals on extended leave (more than 30 days) should be disabled.

(B) Remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.
(C) Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.
(D) Periodically review existing accounts for validity (at least once every 6 months).
(E) Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

(i) Incident Response Policy.
(i) Any breach in the security of background check information, including compromised passwords or missing hardware, must be immediately be reported to the Vice President of Administrative Services.
(ii) Dixie Tech 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.
(iii) The College's Cyber Security Response Team, consisting of the IT Manager, Vice President of Administrative Services and Security, shall develop an incident response plan.

(j) Digital Media Protection Policy. Background check data shall be stored on a secure drive in an encrypted electronic file which is only accessible to the person(s) designated to review them. Background check information must be transmitted only in a secure or encrypted format.

Revision Dates: November 2, 2022; March 2, 2022; March 24, 2020