



## Ohio Administrative Code

### Rule 3358:5-11-21 Identity theft prevention program policy.

Effective: November 15, 2022

---

(A) Program adoption Clark state college developed this identity theft prevention program pursuant to the federal trade commissions red flags rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. After consideration of the size and complexity of the colleges operations and account systems, and the nature and scope of the colleges activities, the Clark state community college board of trustees determined that this program was appropriate for the college and therefore approved this program on March 17, 2009.

#### (B) Definitions

(1) Identity theft a fraud committed or attempted using the identifying information of another person without authority.

(2) Red flag a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(3) Covered account all accounts or loans that are administered by the college.

(4) Program administrator the individual designated with primary responsibility for oversight of the program.

(5) Identifying information any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government-issued drivers license or identification number, alien registration number, government passport number, employer or taxpayer identification number, personal identification number or computer internet protocol address, and bank routing code.

(C) Fulfilling requirements of the red flags rule - Under the red flags rule, the college is required to establish an identity theft prevention program tailored to its size, complexity and the nature of its



operation. Each program must contain reasonable policies and procedures to:

- (1) Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the program.
- (2) Detect red flags that have been incorporated into the program.
- (3) Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.
- (4) Ensure the program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from identity theft.