Ohio Administrative Code

Rule 3309-1-69 Cybersecurity incident notification responsibilities.

Effective: August 4, 2024

(A) For the purposes of this rule:

(1) A "cybersecurity incident" means a cybersecurity event that has been determined to have an impact on the employer prompting the need for response and recovery. This may include ransomware that may place a school employees retirement system member's personal data at risk or an employer business email compromise that may place a school employees retirement system member's personal data at risk.

(2) "Personal data" means full legal name, date of birth, home address, email address, social security number, driver's license number, state identification card number, school employees retirement system account username, school employees retirement system account password, record of contributions or financial account numbers.

(B) Within seventy-two hours of discovery of a cybersecurity incident, an employer shall provide notification of the cybersecurity incident to school employees retirement system by telephone or email. Notification shall be sent to employer services personnel at 1-877-213-0861 or employerservices@ohsers.org. The employer shall also provide the following information within seventy-two hours of discovery of a cybersecurity incident:

(1) The date and time of the discovery of the cybersecurity incident.

(2) The name of the employer cybersecurity incident representative and contact information.

(C) The employer shall provide the following information to employer services regarding a cybersecurity incident within a reasonable period of time:

(1) Date and time of the cybersecurity incident.

(2) Nature of the cybersecurity incident, including any potential impact on school employees retirement system member's personal data or email communications from employer.

(3) Description of personal data involved in the cybersecurity incident.

(4) Employer action taken to mitigate the cybersecurity incident and secure compromised systems.