

**18 NCAC 07J .0627      CYBERSECURITY INCIDENT RESPONSE**

A technology provider shall:

- (1) detect and respond to any cybersecurity incident;
- (2) store evidence related to a cybersecurity incident in a manner that:
  - (a) establishes chain of custody; and
  - (b) preserves chain of custody; and
- (3) retain security logs and other data related to cybersecurity incidents and response for at least three years.

*History Note:* Authority G.S. 10B-4; 10B-106; 10B-125(b); 10B-126; 10B-134.15; 10B-134.17; 10B-134.19; 10B-134.21; 10B-134.23;  
Eff. July 1, 2025.