Non-Instructional/Business Operations

SUBJECT: CYBERSECURITY INCIDENT RESPONSE

The District is committed to providing a timely and comprehensive response to any cybersecurity incident or demand of ransom payment, in accordance with all applicable laws and regulations.

Definitions

For the purposes of this policy, the following definitions apply:

a) "Cybersecurity incident" means an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

b) "Ransom payment" means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

Identifying and Determining the Scope of Cybersecurity Incidents

District personnel must report any suspected cybersecurity incident to their immediate supervisor or manager or to the appropriate district information technology staff. In the event that the incident includes a breach of personally identifiable information (PII), all applicable laws and regulations regarding PII must be followed.

Reporting of Cybersecurity Incidents

The District will report all cybersecurity incidents and/or demand of ransom payments to the commissioner of the division of homeland security and emergency services using the reporting forms at the Division of Homeland Security and Emergency Services Cybersecurity Incident and Ransom Payment Reporting website (https://www.dhses.ny.gov/cybersecurity-incident-and-ransom-payment-reporting). This report must:

a) Include whether the District is requesting or declining advice and/or technical assistance from the division of homeland security and emergency services in relation to the reported cybersecurity incident or demand for a ransom payment; and

b) Be filed no later than 72 hours after the District reasonably believes the cybersecurity incident has occurred.

These reports and any records related to ransom payments submitted to the commissioner of the division of homeland security and emergency services are exempt from disclosure under the Freedom of Information Law (FOIL).

(Continued)

SUBJECT: CYBERSECURITY INCIDENT RESPONSE (Cont'd.)

Notice and Explanation of Ransom Payment(s)

In the event that the District makes a ransom payment in connection with a cybersecurity incident, the District will provide the commissioner of the division of homeland security and emergency services with the following information:

a) Notice of the payment within 24 hours of the ransom payment; and

b) A written description within 30 days of the ransom payment, to include:

1. The reasons the payment was necessary;
2. The amount of the payment;
3. The means by which the payment was made;
4. A description of the alternatives to payment that were considered; and
5. A description of the diligence performed to find alternatives to payment and to ensure compliance with applicable rules, laws, and regulations.

General Municipal Law Article 19 Section 995

Adoption Date: 2/9/26