ANNUAL EMPLOYEE TRAINING

Educational agencies shall **annually provide data privacy and security awareness training** to their officers and **employees with access to personally identifiable information**. Training should include training on the state and federal laws, and how employees can comply with such laws. To learn more about this requirement, agencies can review Part 121.5 and 121.7 of the Regulations.

SUGGESTED PRIVACY AND SECURITY AWARENESS TRAINING TOPICS

LAWS, POLICIES, AND PROCEDURES

- Data Security and Privacy Policy
- Incident Reporting
- Laws and Regulations
- Click Wrap Agreements

SECURITY AWARENESS

- Common Threats
- Phishing Recognition
- Social Engineering

K-12 THREAT LANDSCAPE

As educational agencies assess employee training needs, the most prominent NYS K-12 threat categories should be considered. This information can also inform agencies' NIST align Cybersecurity Action Plans.

SYSTEM AVAILABILITY	DATA INTEGRITY	UNAUTHORIZED PII DISCLOSURE	FINANCIAL THEFT
			
Access to systems or infrastructure is disrupted or denied	Unauthorized data modification causing inaccuracy of information	PII viewed by unauthorized persons via theft or accidental leakage	Monetary loss due to digital theft, social engineering, or extortion

These four areas were identified based on information from the following resources: Verizon Data Breach Investigations Report, Gartner Research, Homeland Security/US-Cert/CIS/MS-ISAC, NYS Troopers, FBI, NYS Office of Information Technology Services, NYS Comptroller Audit Findings, K-12 Cybersecurity Resource Center, PTAC, CoSN, Ponemon Institute Cost of Data Breach Report, Microsoft Security Intelligence Report, Data Quality Campaign, Statewide RIC Data, and Global News Outlets.