DATA SECURITY AND PRIVACY STANDARDS
FOR NEW YORK STATE EDUCATIONAL AGENCIES

NIST CSF DISTRICT READINESS TOOL

DEVELOPED BY:

RIC one
TWELVE REGIONAL INFORMATION CENTERS WORKING AS ONE

VERSION DATE:

November 2019

NYS RICS OVERVIEW:

12 NYS centers organized under and supporting the 37 BOCES to provide shared technology services.

INTRODUCTION TO THE NIST CYBERSECURITY FRAMEWORK

NATIONAL DATA SECURITY FRAMEWORK OVERVIEW

Education Law 2-d requires educational agencies to adopt a policy on data security and privacy that aligns with the state's data security and privacy standard. The Department adopted the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) as the standard for educational agencies. **At the center of the framework is the Core, which is a set of activities and desired outcomes designed to help organizations manage data security and privacy risk**. The Core is organized into functions, categories, and subcategories.

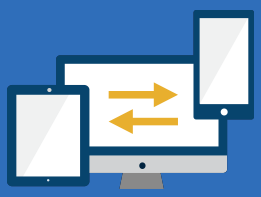
FRAMEWORK CORE 5 FUNCTIONS AND 23 CATEGORIES

IDENTIFY	ASSET MANAGEMENT	BUSINESS ENVIRONMENT	GOVERNANCE	RISK ASSESSMENT	RISK MANAGEMENT STRATEGY	SUPPLY CHAIN
PROTECT	ACCESS CONTROL	AWARENESS AND TRAINING	DATA SECURITY	INFORMATION PROTECTION	MAINTENANCE	PROTECTIVE TECHNOLOGY
DETECT	ANOMALIES AND EVENTS	SECURITY MONITORING	DETECTION PROCESSES			
RESPOND	RESPONSE PLANNING	COMMUNICATIONS	ANALYSIS	MITIGATION	IMPROVEMENTS	
RECOVER	RECOVERY PLANNING	IMPROVEMENTS	COMMUNICATIONS			

IDENTIFY FUNCTION

Develop an **ORGANIZATIONAL UNDERSTANDING TO MANAGE CYBERSECURITY RISK** to systems, people, assets, data, and capabilities.

ASSET MANAGEMENT



ID.AM-1	**Physical devices inventoried**	
ID.AM-2	**Software platforms inventoried**	Potential fields include: system name, vendor, system type, implementation scope, data type, implementation and termination dates, host location, back up practices, maintenance management, log review, security monitoring, data destruction practices, contractual protections
ID.AM-3	**Data flows mapped**	
ID.AM-4	**External systems catalogued**	
ID.AM-5	**Resources prioritized based on classification, criticality, and business value**	
ID.AM-6	**Cybersecurity responsibilities established**	

BUSINESS ENVIRONMENT

ID.BE-1	**Role in the supply chain identified**	
ID.BE-2	**Place in the industry sector identified**	
ID.BE-3	**Organizational objectives established**	
ID.BE-4	**Critical functions established**	
ID.BE-5	**Resilience requirements established**	

GOVERNANCE

ID.GV-1	**Cybersecurity policy established**	As required by Part 121, by October 1, 2020, each educational agency shall adopt and publish a policy that aligns with the NIST CSF
ID.GV-2	**Responsibilities coordinated**	
ID.GV-3	**Legal and regulatory requirements managed**	
ID.GV-4	**Risk management processes address risks**	

IDENTIFY FUNCTION

Develop an **ORGANIZATIONAL UNDERSTANDING TO MANAGE CYBERSECURITY RISK** to systems, people, assets, data, and capabilities.

RISK ASSESSMENT

ID.RA-1	**Vulnerabilities documented**	
ID.RA-2	**Cyber threat intelligence received**	
ID.RA-3	**Threats identified and documented**	Threats impacting the education sector include: system availability (ransomware and DDoS), data integrity (malicious insiders), unauthorized PII disclosure (third-party breaches), fiscal loss or theft (spear phishing)
ID.RA-4	**Organizational impacts identified**	
ID.RA-5	**Threats, vulnerabilities, likelihoods, and impacts used to determine risk**	
ID.RA-6	**Risk responses identified**	

RISK MANAGEMENT

ID.RM-1	**Risk management processes established**	
ID.RM-2	**Risk tolerance determined**	
ID.RM-3	**Risk tolerance informed by sector specific risk analysis**	

SUPPLY CHAIN

ID.SC-1	**Supply chain risk management processes agreed to**	
ID.SC-2	**Third party partners are identified, prioritized, and assessed**	
ID.SC-3	**Contracts are used to implement Supply Chain Risk Management Plan**	As required by Education Law 2-D and Part 121, whenever an educational agency discloses PII to a third-party contractor, the agency must ensure that the agreement for using the product or services includes required language
ID.SC-4	**Third-party partners routinely assessed to contractual obligations**	
ID.SC-5	**Response and recovery testing with third-party providers**	

PROTECT FUNCTION

Develop and **IMPLEMENT APPROPRIATE SAFEGUARDS** to ensure delivery of critical services.

ACCESS CONTROL

PR.AC-1	**Identities managed**	
PR.AC-2	**Physical access to assets managed**	
PR.AC-3	**Remote access managed**	
PR.AC-4	**Permissions managed**	
PR.AC-5	**Network integrity protected**	
PR.AC-6	**Identities proofed**	
PR.AC-7	**Authenticated commensurate with risk**	

AWARENESS AND TRAINING

PR.AT-1	**Users trained**	As required by Part 121, agencies must provide annual awareness training to their officers and employees with access to personally identifiable information
PR.AT-2	**Privileged users understand roles**	
PR.AT-3	**Third-party stakeholders understand responsibilities**	As required by Education Law 2-d, third party contractors and assignees who have access to protected data must receive training on the federal and state law governing confidentiality
PR.AT-4	**Senior executives understand roles**	
PR.AT-5	**Cybersecurity personnel understand responsibilities**	

DATA SECURITY

PR.DS-1	**Data-at-rest protected**	
PR.DS-2	**Data-in-transit protected**	
PR.DS-3	**Assets managed throughout removal**	
PR.DS-4	**Capacity to ensure availability is maintained**	
PR.DS-5	**Protections against data leaks**	
PR.DS-6	**Integrity checking software and information integrity**	
PR.DS-7	**Testing environment(s) separate from production**	
PR.DS-8	**Integrity checking hardware integrity**	

PROTECT FUNCTION

Develop and **IMPLEMENT APPROPRIATE SAFEGUARDS** to ensure delivery of critical services.

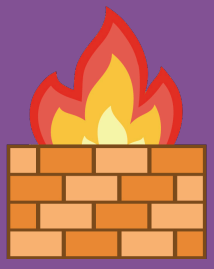
INFORMATION PROTECTION

PR.IP-1	**Baseline configuration created and maintained**	
PR.IP-2	**System Development Life Cycle implemented**	
PR.IP-3	**Configuration change processes**	
PR.IP-4	**Backups conducted, maintained, and tested**	
PR.IP-5	**Physical operating environment met**	
PR.IP-6	**Data destroyed according to policy**	The ED-1 Records Retention and Disposition Schedule indicates the minimum length of time that officials must retain records before they may be disposed of legally
PR.IP-7	**Protection processes improved**	
PR.IP-8	**Effectiveness of protection shared**	
PR.IP-9	**Response plans and recovery plans in place**	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) should include Part 121 reporting and notification requirements
PR.IP-10	**Response and recovery plans tested**	
PR.IP-11	**human resources practices**	
PR.IP-12	**vulnerability management plan implemented**	

MAINTENANCE

PR.MA-1	**Maintenance performed and logged**	
PR.MA-2	**Remote maintenance approved**	

PROTECTIVE TECHNOLOGY



PR.PT-1	**Audit/log records reviewed**	
PR.PT-2	**Removable media protected and restricted**	
PR.PT-3	**Principle of least functionality**	
PR.PT-4	**Communications and control networks protected**	
PR.PT-5	**Mechanisms implemented to achieve resilience**	

DETECT FUNCTION

Develop and implement appropriate activities to **IDENTIFY THE OCCURRENCE OF A CYBERSECURITY EVENT**.

ANOMALIES AND EVENTS

DE.AE-1	**Network operations and expected data flows managed**	
DE.AE-2	**Detected events analyzed**	NYSED requests that agencies compromised with ransomware immediately contact the NYS Intelligence Center, the local District Superintendent, the local RIC Director, and the NYSED CPO
DE.AE-3	**Event correlated**	
DE.AE-4	**Impact of events determined**	
DE.AE-5	**Alert thresholds established**	

SECURITY MONITORING

DE.CM-1	**Network monitored**	
DE.CM-2	**Physical environment monitored**	
DE.CM-3	**Personnel activity monitored**	
DE.CM-4	**Malicious code detected**	Anti-virus solutions that utilize behavioral analysis and artificial intelligence are more effective than definition based systems
DE.CM-5	**Unauthorized mobile code detected**	
DE.CM-6	**External service provider activity monitored**	
DE.CM-7	**Monitoring for unauthorized connections**	
DE.CM-8	**Vulnerability scans performed**	

DETECTION PROCESSES

DE.DP-1	**Responsibilities for detection defined**	
DE.DP-2	**Detection activities comply with requirements**	
DE.DP-3	**Detection processes tested**	
DE.DP-4	**Event detection information communicated**	
DE.DP-5	**Processes continuously improved**	

RESPOND FUNCTION

Develop and implement appropriate activities to **TAKE ACTION REGARDING A DETECTED CYBERSECURITY INCIDENT**.

RESPONSE PLANNING

RS.RP-1	**Response plan executed**	

COMMUNICATION

RS.CO-1	**Personnel know roles**	
RS.CO-2	**Incidents reported**	As required by Part 121, agencies shall report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the CPO within 10 calendar days
RS.CO-3	**Information shared**	As required by Part 121, agencies shall notify affected parents, eligible students, teachers and/or principals no more than 60 calendar days after the discovery of a breach or unauthorized release
RS.CO-4	**Coordination with stakeholders**	
RS.CO-5	**Voluntary information sharing**	

ANALYSIS

RS.AN-1	**Notifications from detection systems investigated**	
RS.AN-2	**Impact of the incident understood**	
RS.AN-3	**Forensics performed**	
RS.AN-4	**Incidents are categorized**	
RS.AN-5	**Processes established to respond to vulnerabilities**	

MITIGATION

RS.MI-1	**Incidents contained**	
RS.MI-2	**Incidents mitigated**	
RS.MI-3	**Newly identified vulnerabilities mitigated**	

IMPROVEMENTS

RS.IM-1	**Response plans incorporate lessons**	
RS.IM-2	**Response strategies updated**	

RECOVER FUNCTION

Develop and implement appropriate activities to **MAINTAIN PLANS FOR RESILIENCE AND TO RESTORE ANY CAPABILITIES** or services that were impaired due to a cybersecurity incident.

RECOVERY PLANNING

RC.RP-1	**Recovery plan executed**	Ensure backups for critical systems are in place, isolated, and protected. Audit backups for completion and functionality. Backups have been critical to ransomware recovery planning.

IMPROVEMENTS

RC.IM-1	**Recovery plans incorporate lessons**	Agencies should make an intentional decision regarding cyber insurance needs.
RC.IM-2	**Recovery strategies updated**	

COMMUNICATIONS

RC.CO-1	**Public relations managed**	
RC.CO-2	**Reputation repaired**	
RC.CO-3	**Recovery activities communicated**	


RIC
one
TWELVE REGIONAL INFORMATION CENTERS WORKING AS ONE