OSS
ORGANIZATION OF
SELF-INSURED SCHOOLS

AP KEENAN & ASSOCIATES

DATA SECURITY & RECOVERY POLICY

It shall be the policy of the Organization of Self-Insured Schools for Property and Liability (the Authority) to have the Authority's data stored in a secure environment in accordance with the following standards:

1) *Non-Electronic Documents*

All Non-electronic data/documents 18 months or older to be scanned and electronically warehoused at a secure location separately from the administrators.

OR

Non-electronic data/documents (Originals) warehoused at a secure location separate from the administrators, until destroyed in accordance with the Authority's Records Retention & Destruction Policy & Procedure.

2) *Electronic Documents*

The Authority's electronic data/documents must be handled by all providers in a secure environment in accordance with the following processes, policies, and standards:

a) Establish and maintain a comprehensive General Computing and Security Policy that:

- Clearly states the responsibilities of personnel with regard to appropriate use and care for the Authority's data
- Clearly defines a strong password policy and supporting standard
- All personnel have attended security awareness training

b) Maintain appropriate security checks and balances for the environments through:

- Complete security assessment and remediation, by industry respected third party
- Annual computer system vulnerability assessments
- Appointed Compliance Officer and Information Security Team
- Maintaining Authority documents in an imaged and Optical Character Recognition (OCR) indexed system with searchable database

c) Maintain secure operations involving Authority data by:

- Provisioning servers that are built to a secure standard and housed in a physically secure location as described below
- Maintaining centrally managed and administered access rights for access to network resources, applications, and data, that restrict access based on needs and appropriate approval
- Using only secure file transfer protocols and/or Pretty Good Privacy (PGP) encryption for any external file transfers of "sensitive" data
- Deploying and maintaining antivirus and anti-malware systems for servers, desktops, and laptops
- Deploying and maintaining hard drive encryption on all desktop and laptop endpoints
- Deploying and maintaining an effective anti-spam system for email to limit the attack vectors available to malware and viruses

- Making secure email (encrypted mail) services available for transfers of sensitive information via email
- Maintaining secure network perimeter and Firewalled DMZ (Demilitarized Zone)
- Having an Intrusion Detection/ Prevention System (IDS/IPS)
- Network monitoring and escalation with 24/7 response
- Installing and maintaining a Virtual Private Network (VPN) solution to control external access along with comprehensive policies for both internal users' and contractor's access and responsibilities
- A secured computer facility with:
    - A security system with restricted physical access
    - An adequate fire suppression system (Gas)
    - An uninterruptable power system (battery failover)
    - Adequate cooling and Heating, Ventilation & Air Conditioning (HVAC) systems
- Protection of data as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as applicable

d) Maintain adequate Business Continuity Plan (BCP) and Disaster Recovery (DR) plan for Information Technology (IT) which:

- Ensures adequate facilities are reserved to relocate core operations and recover:
    - Data & IT Support Services (Recovery Time Objective 1 Week)
    - Data Transfer Services (RTO 2 Weeks)
    - Check Printing Services (RTO 2 Weeks)
    - Client reporting (RTO 3 Weeks)
    - IT Development and Maintenance (RTO 60 Days)

e) Maintain adequate Data Backup and recovery processes that:

- Ensure production data is backed up:
    - "Incremental" daily backups with two weeks retention
    - Weekly "Full" backups
    - Monthly copies of full backups, with 2 months retention
    - End of fiscal year and end of calendar year backups retained for 3 years
    - A running copy of all daily incremental backups is retained on disk/on site for two weeks worth of data
    - Utilize secure off-site services for encrypted backup tape protection picked up daily
    - Maintain encrypted backup tapes
    - Bar-code tapes and record in a database for expeditious retrieval

ADOPTED:

Dated: 10/12/22

ORGANIZATION OF SELF-INSURED SCHOOLS (OSS)

Kraig Magnussen, OSS President