CNMI SLDS

CHALLENGE

PSS does not have a process for securing physical data files in the case of a disaster - like a typhoon. (CDI #4)

- PSS recently incurred considerable damage to buildings and physical data records during Super-Typhoons Soudelor and Yutu
- PSS needs to have consistent procedures to secure physical data records.

SOLUTION

A physical data security solution is attached for approval

- Standard Operating Procedures (SOP's) for schools and central office programs
- Regulation amendment to 60-20-905

OUTCOME

Schools and Central Offices will have centralized and consistent practices regarding storage of physical data files in the event of a disaster.

PSS Central and School Leadership will have important information on safe and secure storage methods and location of physical data records.

CALL TO ACTION:

1. Ammend regulation 60-20-905 to include student educational records.
2. Implement SOP's for schools and central office to secure physical files.

(a) All financial records, inclusive of electronically created or scanned documents, of the PSS shall be retained **and secured physically** *until the completion and close of the audit for the fiscal year to which the records relate or until five years after the completion of the last activity related to the record, whichever is longer, unless a longer period is provided for by law.*
(b) All performance/program records, inclusive of electronically created or scanned documents, required by federal grants or by the PSS shall be retained **and secured physically** *for five years after the last activity related to the record, unless a longer term is provided by law.*
(c) All student educational records, as defined by Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), shall be secured physically for five years after the last activity related to the record, unless physical record has been digitized, or as specified in the CNMI PSS Educational and Office Record Retention Manual, or unless a longer term is provided by law.

Securing Physical Data Solution

1. Project Summary.

   The CNMI Public School System does not have a process for securing physical data files in the case of a disaster, such as a typhoon. (Linked to SLDS Data Security & Privacy Question # 8.5)

2. Background.

   In 2015 and 2018, the CNMI experienced the destruction of Super Typhoons Soudelor and Yutu that devastated the PSS offices and school structures. With many files destroyed and in some cases, scattered all over the offices and campuses, there has been a pending need to have policies and practices in place to secure files that contain confidential or sensitive information of both students and staff in the case of another disaster.

   In addition, the US Department of Education (USDOE) requires that all State Education Agencies (SEA) establish policies and procedures to ensure the continuity of data services in the event of a data breach, loss, or other disaster. Therefore, the Data Governance Committee has identified and prioritized the following critical data issue as an immediate need for PSS: "Develop a process for securing physical data files in the case of a disaster, such as a typhoon."

   The committee will "Develop a process for securing physical data files in the case of a disaster, weather elements, data breach and theft."

3. CNMI Administrative Code, Part 900 - Other Requirements § 60-20-905 Retention of Records/Audit states:

   (a) All financial records, inclusive of electronically created or scanned documents, of the PSS shall be retained until the completion and close of the audit for the fiscal year to which the records relate or until five years after the completion of the last activity related to the record, whichever is longer, unless a longer period is provided for by law.

   (b) All performance/program records, inclusive of electronically created or scanned documents, required by federal grants or by the PSS shall be retained for five years after the last activity related to the record, unless a longer term is provided by law. Modified, 1 CMC § 3806(b), (f), (g).

   History: Amdts Adopted 36 Com. Reg. 35891 (Dec. 28, 2014); Amdts Proposed 32 Com. Reg. 35634 (Oct. 28, 2014); Amdts Adopted 19 Com. Reg. 15449 (Aug. 15, 1997); Amdts Proposed 18 Com. Reg. 14484 (Nov. 15, 1996). Commission Comment: The August 1997 amendments added this new section as "regulation 1010." The Commission created part 900 and codified the provisions of regulation 1010 in this part. The Commission struck the figure "5" from subsections (a) and (b) pursuant to 1 CMC § 3806(e).

4. Storage Recommendations
    4.1. Does NOT have physical storage solutions
        4.1.1. Identify a room or container
        4.1.2. Identify storage type: cardboard box, plastic bin, and/or filing cabinet
        4.1.3. Secure funding
    4.2. Has physical storage solutions
        4.2.1. Rank files according to the classification system of the CNMI Data Breach Plan (e.g. Public, Confidential/Internal, Highly Confidential)
        4.2.2. Documents have to be protected from any kind of theft. Recommend For this purpose security guards or CCTV cameras are kept.
        4.2.3. Powder based Fire extinguishers are also kept which might be needed in case of a fire emergency. Foam or Water based extinguishers are not used because they would damage the paper files.
        4.2.4. To save the boxes from rodents or any kind of insects, pest control is carried out at regular intervals. A yearly Pest Control Contract is maintained. Under this contract Pest Control is carried out in the physical storage every 3 months. Special medicine is used for rodents and termite.
        4.2.5. We take special care to ensure no water leakages occur from the ceiling, doors or windows, especially during the rainy season. For this purpose a product called Multipurpose Sealant is used on all the doors and windows, to ensure all cracks and openings are securely sealed.
        4.2.6. Any electrical device which is defective is removed from the physical storage because it could lead to short circuits.
        4.2.7. All doors and windows are kept shut at all times. At night all doors are locked and checked as well.
        4.2.8. Cleaning is carried out quarterly in the physical storage. This prevents any dust or dirt from coming in contact with the boxes which could damage the documents.
        4.2.9. A school administrator or program director and facilities development management visits once per quarter and monitors for cleanliness, health of the boxes, and structural integrity of physical storage
    4.3. Transferring Files to Network Attached Storage (NAS)
        4.3.1. Each program/department/school will create Standard Operating Procedures (SOP) for digitizing files. Their SOP should list the documents required to be digitized, including but not limited to documents required for audits and reviews.
        4.3.2. Store files according to the classification system of the CNMI Data Breach Plan (e.g. Public, Confidential/Internal, Highly Confidential)
        4.3.3. Store these digital files on an external solution such as Network-attached Storage (NAS, e.g. Synology). In the event NAS has not been procured, digital copies should be stored on external hard drive, flash drive, or cloud storage.
            4.3.3.1. Store digital copies or NAS of your documents offsite in case of physical damage to your office/school.
            4.3.3.2. External hard drives should be securely stored in a locked fire and weather resistant cabinet or storage area.
        4.3.4. Standardized file-naming conventions:
            4.3.4.1. Keep file names short but meaningful
            4.3.4.2. Include any unique identifiers, e.g. Student ID #, PO#, project title, program/school abbreviation, and document name
            4.3.4.3. Be consistent
            4.3.4.4. Indicate date or version number where appropriate
            4.3.4.5. Ensure the purpose of the document is quickly and easily identifiable
        4.3.5. Back-up files regularly.
            4.3.5.1. NAS stored offsite will be configured to back up nightly.
            4.3.5.2. Non-NAS should be backed up regularly. 30-days should not pass for back-up.

5. Regulation Proposal (**proposal in changes are in bold**)

Part 900 - Other Requirements

§ 60-20-905 Retention of Records/Audit

(a) All financial records, inclusive of electronically created or scanned documents, of the PSS shall be retained until the completion and close of the audit for the fiscal year to which the records relate or until five years after the completion of the last activity related to the record, whichever is longer, unless a longer period is provided for by law.

(b) All performance/program records, inclusive of electronically created or scanned documents, required by federal grants or by the PSS shall be retained for five years after the last activity related to the record, unless a longer term is provided by law.

Modified, 1 CMC § 3806(b), (f), (g).

History: Amdts Adopted 36 Com. Reg. 35891 (Dec. 28, 2014); Amdts Proposed 32 Com. Reg. 35634 (Oct. 28, 2014); Amdts Adopted 19 Com. Reg. 15449 (Aug. 15, 1997); Amdts Proposed 18 Com. Reg. 14484 (Nov. 15, 1996).

Commission Comment: The August 1997 amendments added this new section as "regulation 1010." The Commission created part 900 and codified the provisions of regulation 1010 in this part. The Commission struck the figure "5" from subsections (a) and (b) pursuant to 1 CMC § 3806(e).

5.1. All financial records, performance/program records, and inclusive of *(a) All financial records, inclusive of electronically created or scanned documents, of the PSS shall be retained* **and secured physically** *until the completion and close of the audit for the fiscal year to which the records relate or until five years after the completion of the last activity related to the record, whichever is longer, unless a longer period is provided for by law.*

5.2. *(b) All performance/program records, inclusive of electronically created or scanned documents, required by federal grants or by the PSS shall be retained* **and secured physically** *for five years after the last activity related to the record, unless a longer term is provided by law.*

5.3. ***(c) All* student educational records,„ *as defined by Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), shall be secured physically for five years after the last activity related to the record, unless physical record has been digitized, or as specified in the CNMI PSS Educational and Office Record Retention Manual, or unless a longer term is provided by law.***