BUSINESS CONTINUITY AND TECHNOLOGY DISASTER RECOVERY

The Terrebonne Parish School Board recognizes the importance of maintaining and protecting computer hardware and software, including necessary equipment and supplies to maintain computer operations in the event of a disaster. The School Board shall authorize the Superintendent and/or his/her designee to maintain appropriate regulations and procedures for the proper usage of School Board owned or leased computer equipment and the protection of electronic media, applications, and stored user data.

Such regulations and procedures shall assure that:

1. All electronic devices (computers, servers, mobile devices, printers, appliances, etc.) receive available system and software patches, firmware and other updates in a timely manner.

2. All electronic devices (computers, servers, mobile devices, tablets, etc.) should have licensed anti-virus software and be automatically updated daily by the software vendor where applicable.

3. Data critical to daily operations is identified and documented.

4. Backup frequency objectives are clearly defined and procedures are in place to verify the backups are occurring.

5. Backups may be stored locally but should also reside in a separate physical location isolated from the local network where backups are occurring (offsite and/or cloud, etc.).

6. Periodic testing and verification should be performed to ensure that backups can be restored within the recovery time objective (RTO) as defined by the School Board.

7. A *Business Continuity and Technology Disaster Recovery Plan* shall be created that clearly establishes actions to be taken before, during, and after an occurrence, undesirable event, or disaster. The Plan shall be developed, defined, and tested at regular intervals in order to restore critical functions and reestablish normal operations within the RTO (Recovery Time Objective) established by the School Board.

PATCH MANAGEMENT

The security of computer systems is critical to the continued operations of the School Board. A consistent and comprehensive patch management procedure will substantially reduce risks such as viruses, malware, ransomware, and various cyber-crimes that target un-patched systems. Patch management shall be handled in accordance with the standard procedures outlined in the *Business Continuity and Technology Disaster Recovery Plan*. Exceptions to the standard procedure may be permitted when justified. Any exceptions must be fully documented. The standard procedure for patch management shall include the following:

- Identification of the systems and devices to be patched and updated and are documented and regularly reviewed/verified. Devices to be patched shall include computers, servers, mobile devices, tablets, printers, appliances and other devices as established by the Technology Department.

- Software and procedures to identify and apply patches, security updates, drivers and firmware are documented and regularly reviewed/verified.

- Patch management frequency is clearly documented and procedures and/or reporting shall verify that updates are occurring at the established intervals.

ANTI-VIRUS

A comprehensive anti-virus deployment substantially reduces risks such as viruses, malware, ransomware, and various cyber-crimes that target systems without protection. Anti-virus deployment shall be handled in accordance with the standard procedures outlined in the *Business Continuity and Technology Disaster Recovery Plan*. Exceptions to the standard procedures may be permitted when justified. Any exceptions shall be fully documented. The standard procedure for anti-virus deployment shall include the following:

- Identification of the systems and devices that are capable of running anti-virus software shall be documented and regularly reviewed/verified.

- Systems capable of running anti-virus software shall include computers, servers, mobile devices and tablets, and other devices as established by the Technology Department.

- The Technology Department shall be responsible to identify and adopt an anti-virus platform that is consistent with secure industry standards. Under no circumstances shall freeware Anti-virus products be used on School Board systems.

- Software and procedures to install anti-virus software, verify system health and automatically apply updates are documented and regularly reviewed/verified.

- The Technology Deportment shall be responsible for regularly performing network scans to identify unprotected systems and adding those systems into the anti-virus deployment.

BACKUP - IDENTIFICATION OF DATA

Important and/or critical data as defined by the Terrebonne Parish School Board in the *Business Continuity and Technology Disaster Recovery Plan* includes the following file types:

- Word processor, spreadsheet, and presentation files used in educational or administrative applications necessary to perform job description duties for the Terrebonne Parish School Board

- Database files used for educational or administrative purposes

- Browser bookmark or favorites; e-mail lists

Picture/movie files such as (.bmp, .jpeg, .jpg, .tiff, .mpeg, .wav, .mp3, etc.) **shall not** be backed up unless special circumstances arise. Permission shall be directed to the Technology Department to request backup of these file types.

BACKUP – FREQUENCY AND STORAGE

Backup of all important and/or critical computer data shall be handled in accordance with the standard procedures outlined by the Technology Department. Exceptions to the standard procedures may be permitted when justified. Any exceptions must be fully documented. The standard procedure for systems backup shall be as follows:

- All student records in the student information system, including special education records, shall be backed up nightly to offsite storage.

- Accounting (Payroll, General Ledger, Accounts Payable, Purchasing, etc.) records shall be backed up daily to on-site, off-site, and disaster recovery off-site backups. In addition, incremental backups shall be done automatically throughout the day to disaster recovery off-site backups.

- Any educational application (all email, drive storage, calendars, and contacts shall be backed up by a third-party company to cloud storage).

- Student, teacher, and administration files are the responsibility of the individual to back up:

    - The School Board recommends backing up to the individual's Google Drive or similar application as approved by the Technology Department. This location should be backed up continuously throughout the day.

    - All servers not managed by a third party shall be backed up daily to the central office backup server Monday through Friday. Servers shall then be backed up on weekends to offsite and archival cloud storage.

BACKUP – VERIFICATION AND TEST RESTORES

The Technology Department shall be responsible for establishing procedures to verify backups and perform test restores on files and systems. The standard procedure for verification and testing shall include:

- Backup verification and test restore objectives shall be clearly defined and procedures are in place to confirm the verifications and test restores are occurring.

- Backup verification shall include regularly reviewing backup selection sets, and confirming that selection sets are complete and correct.

- Backup verification shall also include procedures or reporting to verify that backups are occurring at the established intervals.

- Periodic test restores shall be performed on files and folders and systems where possible in an appropriate test environment (example: sandbox). The interval for test restores shall be clearly defined and procedures are in place to verify the test restores are occurring.

BACKUP – RESTORATION OF FILES

Active files that are accidentally damaged or deleted can normally be restored from backup within one working day provided the Technology Department is notified in a timely manner. Files can only be restored to the state they were in at the time the most recent relevant backup was taken.

Accounting systems can be activated under the *Business Continuity and Technology Disaster Recovery Plan* established with the software vendor in a timeline established by the software vendor.

BUSINESS CONTINUITY AND TECHNOLOGY DISASTER RECOVERY PLAN

In the event of an occurrence, undesirable event or disaster (“event”), the restoration of computing services is critical to the continued operations of the School Board. A *Business Continuity and Technology Disaster Recovery Plan* shall be created that clearly establishes actions in preparation of an event, procedures to follow during an event, and the review and recommendations that should occur after the event. *Business Continuity and Technology Disaster Recovery* shall be handled in accordance with the standard procedures outlined by the Technology Department. Exceptions to the standard procedures may be permitted when justified. Any exceptions must be fully documented and approved by the School Board. The standard procedures for *Business Continuity and Technology Disaster Recovery* shall include:

- Business Impact Analysis (BIA) shall be performed to differentiate critical (urgent) and non-critical (non-urgent) organization functions/activities. A function may be considered critical if dictated by law. For each function, two (2) values shall be assigned: RPO (Recovery Point Objective) and RTO (Recovery Time Objective). A Recovery Point Objective (RPO) shall be assigned to all functions that identifies the acceptable latency of data that will not be recovered (usually based on backup frequency).

- A Recovery Time Objective (RTO) shall be assigned to all functions that identifies the acceptable amount of time to restore the function.

- The Technology Department shall use the results of the BIA to determine which systems and processes are most critical, and what order those systems and processes should be restored. The identification of critical systems and the order of restoration shall be documented and reviewed at regular intervals.

- The Plan shall identify personnel and vendors that will oversee disaster planning, testing and critical recovery efforts during an event, with a clear delineation of responsibilities.

- The Plan shall identify a list of employees, vendors, students, agencies, etc. that should be notified at the onset of an event. The list shall include current contact information including phone and email addresses. A notification procedure should be established and contact information should be verified at regular intervals.

- The Technology Department shall be responsible for establishing an environment for testing the Plan (example: sandbox), and testing should be performed annually at a minimum. The Plan shall be updated, as necessary, to achieve the RPO and RTO objectives, or other objectives as identified by the Technology Department or School Board.

- If an event occurs, the Technology Department shall be responsible to perform a review and analysis (Post Mortem) of the event, and make recommendations to the School Board to prevent such event in the future. The Plan shall be updated as necessary to achieve the RPO and RTO objectives, or other objectives as identified by the Technology Department or School Board.

- The *Business Continuity and Technology Disaster Recovery Plan*, and the results/findings from the latest recovery testing shall be presented to the School Board annually for review and approval.

CYBERSECURITY TRAINING

The School Board shall identify employees or School Board members who have access to the School Board's information technology assets and require those employees and School Board members to complete cybersecurity training. Each School Board member or employee with access to the School Board’s information technology assets shall complete this training within the first thirty (30) days of initial service or employment with the agency.

The Superintendent shall verify and report to the Department of State Civil Service on the completion of cybersecurity training by employees. The Superintendent shall periodically require an internal review to ensure compliance.

The School Board shall require any contractor who has access to School Board information technology assets to complete cybersecurity training during the term of the contract and during any renewal period.

Completion of cybersecurity shall be included in the terms of a contract awarded by a state or local government agency to a contractor who has access to its information technology assets.

The person who oversees contract management for the School Board shall report each such contractor's completion to the Superintendent and periodically review agency contracts to ensure compliance. The Superintendent shall verify and report to the Department of State Civil Service on the completion of cybersecurity training by each such contractor.

New policy: January 2020

Ref: La. Rev. Stat. Ann. §§17:81, 42:1267. Board minutes, 2-2-21