PEDIATRIC NURSING CERTIFICATION BOARD

Security

This Security Policy covers all aspects of the Pediatric Nursing Certification Board's (PNCB's) operations. All employees, volunteers, vendors, and consultants are responsible and held accountable for maintaining the highest level of security.

Confidential Documents

Confidential information is defined in the Confidentiality Policy. All staff, volunteers, vendors and consultants are required to review and acknowledge their role annually by signing an individual agreement or through inclusion via contract. All confidential information will be managed in a secure manner as per PNCB's policy.

Certification exams, job analysis surveys or reports, cut score reports, item banks, answer keys, and all other exam development documents are confidential and the sole property of PNCB.

Access

Access to secure/confidential materials is limited to only those staff, Board members, volunteers, vendors, and consultants who have a valid and approved need to view the information. These individuals will sign a confidentiality agreement and conflict of interest agreement prior to being granted access.

Physical Security

All physical confidential files and documents will be stored in a locked cabinet/file/safe. This material will remain locked up when un-authorized individuals are present. When authorized staff leave the area all confidential materials must be secured.

If there is a need to transport physical confidential information, only traceable methods with tamper evident packaging will be utilized. Staff will seal the material and monitor until receipt by another authorized individual is confirmed.

The PNCB office is secured with both traditional and electronic security devices. Only authorized staff are provided with hard and soft (passwords) access for entry into the premises. Changes to staff status or classification are made by the Chief Executive Officer (CEO), Chief Operating Officer (COO) or designee. The COO has the responsibility of updating access information.

Electronic Security

1. Network Access is restricted to those users who need access to provide service to employees, candidates, certificants and volunteers. Access is controlled by the COO and Network Administrator. User level passwords are required and updates/changes to these are required periodically. No user may use another user's access (enforced by hardware, software, monitoring equipment and supervisors). Multi-factor authentication protocols are utilized as appropriate.
2. Electronic File Transfer – files can only be transferred outside the organization using a secure transfer protocol such as restricted FTP, Secure Share or similar platform.
3. Exam Forms/Item Banking – can only be accessed through vendor-provided platforms that are reviewed and deemed to have met PNCB security requirements (password protected/encrypted etc.).
4. Candidate Data – all candidate data is transferred using a secure transfer protocol. Candidate data storage is secured via user level access passwords and network/data center security (fire walls).

Data Storage
All data files are backed up nightly to an off-site data center. All back-up data storage devices are password protected. Back up data devices and storage are accessible by only by the CEO, their designee, and the Network Administrator.

Records are stored/retained per the Record Retention Policy.

Exam Administration
The security of exams during delivery is the responsibility of the exam delivery vendor. PNCB utilizes a Client Practice document to direct the vendor in administering PNCB exams. Daily reports containing irregularities are received from the vendor and reviewed by PNCB staff prior to score processing. Any incidents reported by the vendor are investigated. Please refer to the Irregular Behavior Policy for additional information.

Security Audits
Security audits are conducted randomly by the CEO, COO and/or their designee.

Security Breach
Any reported, detected or suspected breaches in security are required to be reported immediately to the COO. If the COO is not readily available to receive the report it will go to the CEO. All breaches will be immediately investigated. A report will be provided to the CEO within 24 hours of the event and/or report. Appropriate action plans will be executed. Candidates/certificants are notified if any of their personal data has been exposed.

Date Approved: 11/1/1975, 06/2016
Last Revision Date: 05/2016, 2/28/2021