



Policy for the Appropriate Use of Information Technologies

I. POLICY SCOPE

This Policy applies to all users of the Puerto Rico School of Nurse Anesthetists (PRSNA) Information Technologies (IT), including but not limited to students, faculty and staff. Third parties who use any part of the PRSNA Information Technologies, such as contractors, consultants, or visitors, are also subject to this Policy, including when they connect their own equipment to the PRSNA network or install proprietary software on computers property of PRSNA. Unawareness of the existence of this Policy, does not excuse users from its compliance.

II. OBJECTIVES

The purpose of this policy is to define a normative that enables members of the PRSNA community to make the best use of technology resources in a secure environment that promotes the PRSNA's objectives of transmitting and increasing knowledge through instruction and service. This Policy aims to safeguard the integrity of computers and related equipment, networks, systems, programs, and data, regardless of whether or not these are located on PRSNA grounds; Ensure that use of electronic communications complies with applicable PRSNA, Governmental, federal and international laws, policies, norms, and procedures, and; Protect PRSNA against damaging security and legal consequences.

III. POLICY STATEMENT

Computers, networks and electronic information systems are essential for accomplishing the PRSNA's mission of instruction and service. PRSNA grants members of the academic community shared access to these resources in support of accomplishing the PRSNA's mission. These resources are to be used responsibly to ensure their integrity, security, and availability for appropriate educational, service, and other institutional activities. Users are required to use IT resources effectively and responsibly; in a manner that does not affect the quality or delivery of a person's work to PRSNA nor hamper the rest of the community's ability to conduct their work.

PRSNA values and supports freedom of expression and an open environment for learning and sharing information. Censorship is incompatible with the goals of our institution. Therefore, information accessible from available electronic sources may not be restricted through censorship, as long as this information is not constrained by law or regulations and it is used for lawful purposes. PRSNA will promote the appropriate use of technology, mainly through education, to encourage responsible management of technology and the information that is accessed.

Access to the information resource infrastructure, sharing of information, and security of intellectual products, all require that every user accept personal responsibility for protecting the rights of the community. Users should be aware that actions conducted using information technology will be held to the same standards as any other action in the work place. PRSNA will deal promptly with all violations of any law or institutional policy.

IV. RIGHTS AND RESPONSIBILITIES

Members of the PRSNA community are granted access to information technology resources to facilitate their academic, service, and job activities. Personal use of information technology is not allowed. Assessment of an employee's job performance may consider the employee's personal use of information technology resources; and a supervisor may request a change in this personal use as a condition for continued employment.

A. Acceptance of Policy and Norms

By using PRSNA's IT resources, users agree to abide by this Policy, as well as all relevant PRSNA's policies, norms, and procedures, and current federal and Commonwealth laws. Users are responsible for:

1. Understand, and comply with all policies, procedures and laws related to access, acceptable use, and security of PRSNA's information technologies.
2. Request system administrators for clarification on access and acceptable use of the information technologies.
3. Report possible policy violations to administrators.

B. Privacy and Security

PRSNA recognizes the user's right to privacy and security; and will take reasonable measures to protect their security when using information technologies. The user's personal information will be maintained in a secure environment; and only accessed by authorized employees when necessary. Should the need arise to intervene with a person's right to privacy in the course of any investigation regarding inappropriate use of information or technology resources, PRSNA will do so following existing legal procedures. Users should follow the appropriate security procedures to assist in keeping equipment, systems and accounts secure.

C. Consequences of Violations

Access privileges to PRSNA Information Technologies will not be denied without cause. PRSNA may temporarily deny access to these resources if, during the course of an investigation, it appears necessary to protect the integrity, security, or continued operation of its computers, systems and networks or to protect itself from liability. Alleged violations of PRSNA's policies shall be referred to appropriate PRSNA officials for resolution or disciplinary action. PRSNA may also refer suspected violations of the law to the appropriate law enforcement agencies. Depending upon the nature and severity of the offense, policy violations may result in loss of access privileges, PRSNA disciplinary action, and/or criminal prosecution.

V. PRSNA RIGHTS AND RESPONSIBILITIES

PRSNA owns the applications, systems, computers, and networks that comprise the institutional technological infrastructure. Likewise, PRSNA owns all data that reside on this technical infrastructure; and is responsible for taking the necessary measures to ensure the integrity, security, and confidentiality of its systems, applications, data, and user accounts.

When PRSNA becomes aware of violations, either through routine system administration activities, audits, or from a complaint, it is the institution's responsibility to investigate as needed, and to take whatever necessary actions to protect its resources and/or to provide information relevant to any investigation underway. PRSNA offices and facilities shall cooperate and work alongside appropriate PRSNA and law enforcement officials investigating these violations.

VI. FUNCTIONAL RESPONSIBILITIES

A. Information Technologies Staff

1. IT staff will present recommendations for the acquisition of computers, computer- and network- related equipment, and software, as well as any proposed implementation of information systems or information technology. The IT staff will promptly issue its recommendations on changes, updates, and implementation of the existing or proposed technology, to avoid undue delays.

2. IT staff will protect information technology resources and data. IT staff personnel will treat the content of institutional data, individual assigned accounts, and personal communications as private and will not examine or disclose this content, except: (1) as may be required for system maintenance, including security measures; (2) when there exists a documented reason to believe that an individual is violating the law or PRSNA policy; or (3) as permitted by applicable policy or law.
3. The data registered, maintained, stored, and accessed through the PRSNA's information systems is a critical resource that must be protected. IT staff will ensure that appropriate security measures and standards are implemented and enforced. In case of doubt, IT staff will treat information as confidential until otherwise informed.

VII. EFFECTIVE DATE

This Policy shall be effective immediately after its approval on May 2020.