PNU IT
Information Asset Acceptable Use Policy
Version: 2.1

جامعة الأميرة نورة بنت عبدالرحمن
Princess Nourah Bint Abdulrahman University

PNU, Saudi Arabia

Contents

Document Management Information

Document Title : Information Asset Acceptable Use Policy

Document Owner: PNU ITSM

Security Classification: Internal

The "Information Asset Acceptable Use Policy" is released for the use in Princess Nourah Bint Abdulrahman University (PNU), henceforth referred to as PNU. PNU holds all the rights on this document. No part or full of this document should be replicated or copied. The intended users of this document are all the relevant departments of PNU, the PNU Information Security Committee (PNUISC) and any other support groups who are responsible for Information Security in PNU. This document is subject to the PNU document control procedures. Comments, suggestions, and queries should be addressed to PNUISC/ ISM (Information Security Manager) using the email "ITC-Security@pnu.edu.sa".

1- PURPOSE

The purpose of this policy is to establish rules for acceptable use of technical assets Within the PNU and all entities under PNU .

2- SCOPE

This policy is applicable to all employees, students , consultants, trainees, contractors and Third party individuals and to all information assets within PNU and all entities under PNU .

3- Policy Statement

3.1 General terms:

- All users shall comply with Asset Acceptable Use Policy.
- All users shall be responsible for the protection of PNU owned assets assigned to them for conducting the required activities.
- PNU assets and resources shall not be used for any unlawful, unethical or unauthorized purpose.
- All users shall handle with PNU information's according to the information Classification Policy in PNU to guarantees the protection of confidentiality, integrity and availability of information.
- Users shall comply with copyrights and licensing agreements.
  - Copyrights: Software shall not be copied except as permitted by copyright law or a license agreement. Copyright of material copied from any source shall be explicitly attributed to the copyright owner and clearly displayed.
  - Licences: The number of simultaneous users shall not exceed the number of licenses purchased.
  - Rights in content - do not use third party text, images, sounds, trademarks and logos in materials such as emails, documents and web pages without the consent of the rights holder.
- External storage media must be kept safe and appropriate, such as making sure that the temperature is set to a certain degree and kept in an isolated and safe place.
- Users are not allowed to disclose any information related to PNU , including information related to systems and networks, to any unauthorized party or party, whether internal or external.

- Users are not allowed to use or share other users password, including the password for the departments or mangers .
- The users shall not indulge in unlawful activities such as accessing unauthorized Resources, stealing or misusing a password, hacking, introducing any computer contaminant or computer virus, committing acts, which may disrupt use of the resources, or aiding or abetting any of the above.
- Usage of PNU assets for personal purpose shall be avoided.
- Unauthorized devices shall not be used within the PNU network .
- PNU respects the privacy of the individuals and also desires to provide a reasonable level of privacy. However, PNU may monitor and audit all its equipment, systems, and network and information assets at any time, with or without prior notice for security, compliance, and maintenance purposes.
- Users shall not use PNU network or resources for blogging. Use of PNU name or business information in any form on personal blogs shall be strictly prohibited.
- Users shall not register or post their PNU email addresses on internet unless required for university purpose and authorised by functional head.
- It's not allow to host unauthorized persons to enter sensitive places without obtaining a prior permit .
- identification card must be worn at all facilities
- Any activities intended to bypass the protection systems for PNU, including anti-virus software, firewall, and malware, are prohibited.
- The Cyber security department and Data management officer must be notified in case of loss, theft or leakage of information , by contacting with :
- All data that is created on university systems shall remain the property of PNU

3.2 Acceptable use of Devices :

- Strict restriction on the use and security of external storage media devices.
- It is not allowed to perform any activity that affects the efficiency and safety of systems and assets without prior permission from the PNU, including activities that enable the user to obtain higher privileges.
- All device must be secured before leaving the office by locking the screen, or signing out (Sign out or Lock), whether leaving for a short period or at the end of working hours.
- Users are not allowed to leave any classified information in accessible places, or to view it by unauthorized persons.
- Users are not allowed to install external tools on the computer without prior permission from the information technology department .

- Cyber security shall be notified upon suspicion of any activity that may cause damage to the computers of PNU or its assets.

3.3 Acceptable use of the Internet and software :

- Cyber security department should be informed in case of suspicious websites that should be blocked.
- Users must ensure that intellectual property rights are not violated while downloading information or documents for business purposes.
- Use of unlicensed software or other intellectual property is prohibited.
- You must use a secure and authorized browser to access the Intranet or the Internet.
- Techniques that allow bypassing the proxy or firewall to access the Internet are prohibited.
- The Cyber security department must be informed when a cyber risk is suspected, and security messages that may appear while surfing the Internet or internal networks must be dealt with caution.
- Users are not allowed to conduct a security scan for the purpose of discovering security vulnerabilities, including conducting penetration testing, or monitoring PNU's networks and systems, or networks and systems of third parties.
- Users are not allowed to use external file-sharing websites .
- Users are not allowed to visit suspicious sites, including hacking sites.
- Users are not allowed to download or install software and tools on the assets of PNU without prior permission from the Information technology department .
- Non-business use of the Internet is prohibited, including downloading media
- Any deliberate attempt to alter, harm or destroy for any assets of PNU shall be prohibited. All such acts shall result in initiation of strict disciplinary/ legal action.

3.4 Acceptable use of e-mail and communications system :

- Users are not allowed to use e-mail, telephone, fax or electronic fax for non-business purposes, and in accordance with cyber security policies and standards.
- Users are not allowed to send messages containing inappropriate or unacceptable content, including messages circulated with internal and external parties.
- Encryption techniques must be used when sending sensitive information by e-mail or communication systems.
- The e-mail address of PNU must not be registered on any site that is not related to work.

- Cyber security department must be notified when it is suspected that there are e-mail messages that contain content that may cause damage to PNU's systems or assets.
- PNU have the right to disclose the contents of e-mail messages after obtaining the necessary permits from the authorized person and the Cyber Security Department in accordance with the relevant procedures and regulations.
- All users are not allowed to open suspicious or unexpected emails and attachments even if they appear to be from reliable sources.
- All users shall comply with PNU's Email Policy while using the corporate e-mail facility.

3.5 Video meetings and web-based communications:

- Users are not allowed to use unauthorized tools or software for making video calls or meetings.
- Users are not allowed to conduct non-work-related video calls or meetings without prior authorization.

3.6 Passwords usage :

- Safe passwords must be chosen, and the passwords for assets or admins of PNU systems must be preserved. You should also choose different passwords from the passwords of personal accounts, such as personal mail accounts and social networking sites.
- Users are not allowed to share the password with any , SMS texting , WhatsApp ,voice communication, and paper writing. All users shall not disclose the password to any third party including co-workers and employees of the Information Technology Department.
- The password must be changed, when a new password is provided to you by the system administrator.

4- Enforcement

- All PNU employees, third parties and third-party consultants shall read and abide by this Policy.
- Any user found in violation to this policy shall be subjected to disciplinary action
- The Cyber Security manger must ensure that all PNU user comply with this policy on regular basis .

5- Point of Contact

For any clarification or further information on this policy contact Information Security Manager at "ITC-Security@pnu.edu.sa".

6- Reference

- ISO 27001: Clause A.8.1.3 (Acceptable Use of Assets)