Air Niugini

NETWORK COMPUTING POLICY

Information Technology is responsible for securing the Air Niugini network and computing systems in a reasonable and economically feasible degree against unauthorised access and/or abuse, while making them accessible for authorised and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to them. Any attempt to violate the provisions of this policy will result in disciplinary action in the form of temporary revocation of user accounts, regardless of the success or failure of the attempt. Permanent revocations can result from disciplinary actions taken by a panel judiciary board called upon to investigate network abuses.

The users of the network are responsible for respecting and adhering to local, state, national and international laws. Any attempt to break those laws through the use of the network may result in litigation against the offender by the proper authorities. If such an event should occur, this organisation will fully comply with the authorities to provide any information necessary for the litigation process.

SECTION 1: GENERAL COMPUTING POLICY

Once a user receives a userID to be used to access the network and computer systems on that network, they are solely responsible for all actions taken while using that userID. Therefore:

1.1 Applying for an userid under false pretences is a punishable disciplinary offence.

1.2 Sharing your userid with any other person is prohibited. In the result that you do share your userid with another person, you will be solely responsible for the actions that other person appropriated.

1.3 Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.

1.4 Attempts to evade or change resource quotas are prohibited.

1.5 Continued impedance of other users through mass consumption of system resources, after receipt of a request to cease such activity, is prohibited.

1.6 Use of facilities and/or services for commercial purposes is prohibited.

1.7 Any unauthorised, deliberate action that damages or disrupts a computing system, alters it normal performance, or causes it to malfunction is a violation regardless of system location or time duration.

SECTION 2: ELECTRONIC MAIL POLICY

Whenever you send electronic mail, your name and userid are included in each mail message. You are responsible for all electronic mail originating from your userid. Therefore:

2.1 Forgery (or attempted forgery) of electronic mail messages is prohibited.

2.2 Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.

2.3 Attempts at sending harassing, obscene and/or other threatening e-mail to another user is prohibited.

2.4 Attempts at sending unsolicited junk mail, "for-profit" messages or chain letters is prohibited.

SECTION 3: NETWORK & DATA SECURITY

As a user of the network, you may be allowed to access other networks (and/or the computer systems attached to those networks). Therefore:

3.1 Use of systems and/or networks in attempts to gain unauthorised access to remote systems is prohibited.

3.2 Use of systems and/or networks to connect to other systems, in evasion of the physical limitations of the remote system/local, is prohibited.

3.3 Decryption of system or user passwords is prohibited.

3.4 The copying of system files is prohibited.

3.5 The copying of copyrighted materials, such as third-party software, without the express written permission of the owner or the proper license, is prohibited.

3.6 Intentional attempts to "crash" Network systems or programs are punishable disciplinary offences.

3.7 Any attempts to secure a higher level of privilege on Network systems are punishable disciplinary offences.

3.8 The wilful introduction of computer "viruses" or other disruptive/destructive programs into the organisation network or into external networks is prohibited.

3.9 Only important work related data can/should be placed on a network drive such as the 'X' drive or other designated network folders that are backed up regularly.

4.0 The backup of personal data remains the responsibility of the user and no personal data should be stored on any network drives or folders as they will only take up valuable disk space for genuine work related data.

4.1 Use of personal external storage devices such as 'flash drives', floppy disks etc is prohibited unless prior approval is sought from IT.

Note:

This is to certify that I, ________________________(Please state full name) have read through and understood the "Network Computing Policy" and agree to comply with all the terms and conditions stated above. I also agree to take full responsibility for all my actions while as an active user on the Air Niugini domain and accept any consequences as a result of breaching any of these policies.

________________ ________________ ________________

Signature Staff ID Date