GUIDELINES FOR NETWORK USERS:

I. Accounts and Passwords
The User of a Net Access ID guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used for educational/official purposes. The User guarantees that the Net Access ID will always have a password. The User will not share the password or Net Access ID with anyone. Network ID's will only be established for students, staff and faculty who are currently affiliated with the University.

Students and staff who leave the University will have their Net Access ID and associated files deleted.

No User will be allowed more than one Net Access ID at a time, with the exception that faculty or officers who hold more than one portfolio, are entitled to have Net Access ID related to the functions of that portfolio.

II. Limitations on the use of resources
On behalf of the University, CIS reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

III. Computer Ethics and Etiquette
The User will not attempt to override or break the security of the University computers, networks, or machines/networks accessible there from. Services associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages. Even sending unsolicited bulk e-mail messages comes under IT Policy violation.

In addition, the User agrees to adhere to the guidelines for the use of the particular computer platform that will be used.

User's Net Access ID gives him/her access to e-mail, and campus computing resources. The use of these resources must comply with University policy and applicable. Electronically available information
(1) may not contain copyrighted material or software unless the permission of the copyright owner has been obtained,

(2) may not violate University policy prohibiting sexual harassment,

(3) may not be used for commercial purposes,

(4) should not appear to represent the University without appropriate permission, or to represent others,

(5) may not appear to represent other organizations or companies,

(6) may not contain material which violates pornography laws, or algorithms or software which if transferred violate laws,

(7) may not contain scripts or code that could cause a security breach or permit use of resources in opposition to University policy.

IV. Data Backup, Security, and Disclaimer

CIS or UCMC will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of an CIS/UCMC staff member in the process of helping the user in resolving their network/computer related problems. Although CIS/UCMC make a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access ID, storage space or email Account. In addition, CIS makes no guarantee concerning the security or privacy of a User's electronic messages.

The User agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold CIS or UCMC, as part of JNU, harmless for any such liability or expenses. JNU retains the right to change and update these policies as required without notification to the User.

V. Account Surrendering:

Retiring employees and the students leaving the university (temporarily or permanently) are advised to get their accounts (NET Access and Email) disabled by giving a written letter to CIS. This is essential as the facility is meant only for the serving employees and the enrolled students. Further, in case the accounts are not disabled and misused by some other person unauthorisedly, the account holder would be legally responsible for such misuse of the account. If retiring employees and the students leaving the university (temporarily or permanently) want to retain the facility for some more period, such requests may be considered, if they are given in writing with valid justification and duly recommended by the competent authority.

VI. Account Termination and Appeal Process

Accounts on JNU network systems may be terminated or disabled with little or no notice for any of the reasons stated above or for other

inappropriate use of computing and network resources. When an account is terminated or disabled, CIS will make an attempt to contact the user (at the phone number they have on file with CIS) and notify them of the action and the reason for the action. If the termination of account is of temporary nature, due to inadvertent reasons and are on the grounds of virus infection, account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicates to the CIS of the same. But, if the termination of account is on the grounds of willful breach of IT policies of the university by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may first approach the Director CIS, justifying why this action is not warranted. If the issue is not sorted out he/she may appeal to the Appeals Board duly constituted by the university for this purpose to review the evidence and hear reasons why an appeal should be considered. If the Appeals Board recommends revival of the account, it will be enabled. However, the decision of the Appeals Board is final and should not be contested.

Users may note that the University's Network Security System maintains a history of infractions, if any, for each user account. In case of any termination of User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate University authorities.