system users must recognize the sensitivity of all other passwords and computer or network access information in any form, and must not use, copy, transmit, share or divulge such information, nor convert the same from encrypted or enciphered form to unencrypted form or legible text. Any attempt to conduct such actions by a system user is a violation of this policy.

iii. take re^ uch ŭ ᵀ

Network Resources. System users must not attempt to defeat or subvert security measures. System users must not use any other network address (e.g., IP address) for a Computer or Network Resource than has been properly assigned by an authorized system or network administrator.

x. treat non-University Computer and Network Resources in accordance with this policy. University Computer and Network Resources must not be used to attempt to breach the security or security policy of other sites (either willfully or negligently). An action or attempted action affecting non-University Computer and Network Resources that would violate this policy if performed on University of Central Arkansas Computer and Network Resources is prohibited.

b. System Administrators shall:

Unless otherwise stated, system administrators have the same responsibilities as system users. However, because of their position, system administrators have additional responsibilities and privileges for specific systems or networks.

i. utilize the enterprise authentication credentials provided by IT to provide access to the System Users of each resource under their management. Exceptions to this must be authorized by IT and ISD.

ii. prepare and maintain security procedures that implement University and college/unit security policies in their local environment and that address such details as access control and

Copyright and Intellectual Property:

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violation using University Computer and Network Resources are prohibited. Computer software protected by copyright is not to be copied from, into, or by using University Computer and Network Resources, except as permitted by law or by the license or contract with the owner of the copyright.

Reporting Security Incidents or System Vulnerabilities:

Individuals aware of any breach of information or network security, or compromise of computer or network security safeguards, must report such situations to the appropriate system administrator and to the Information Security Department within 48 hours of discovery. The University Information Security

facilities are unavailable or not feasible, it may be impossible to complete requirements for course work or work responsibility. The University views misuse of computers as a serious matter, and may restrict access to its facilities even if the user is unable to complete course requirements or work responsibilities as a result.

Exceptions And Exemptions

Exception to or exemptions from any provision of this policy must be approved by IT. Similarly, any questions about the contents of this policy, or the applicability of this policy to a particular situation should