2. KSU does not permit authorized users of the campus e-mail system to share their user ID's or passwords.

3. Authorized users of the e-mail system are fully responsible for activity performed by their user ID.

4. Faculty or Staff requesting access to the campus e-mail system must complete a "Request for Network Access" form and forward to their Department Head. IT will base authorization for these user ID's by information supplied on the access form.

5. Each Department Head may delegate responsibilities for authority. They must notify Information Technology of any delegation of authority.

6. Information Technology will administer all authorized access and security for the campus e-mail system.

7. Kentucky State University does not permit authorized users of the campus e-mail system to use the e-mail system except as explicitly stated on their "Request for Network Access" form.

8. Unauthorized use of the e-mail system by an individual not in accords with the mission of Kentucky State University represents a breach of security.

9. Information Technology has the authority to terminate any user's e-mail access if a breach of security occurs or if security is in question.

10. If an authorized user becomes aware of a security breach involving his or her user ID, it is the responsibility of that user to immediately notify their Department Head and Information Technology of the security breach.
When an authorized employee terminates employment with the University his or her operator ID will be disabled or deleted. The supervisor of the organizational unit for which the terminating employee works most notify Information Technology and IT will disable the users ID on the employee's last date of employment with KSU or IT will disable account based on the KSU check out list.

1. E-mail access may be suspended or voided if any unauthorized use of the University e-mail systems occur. This may include, but is not limited to, any unauthorized use of any user ID and password.

Any employee who becomes aware of a breach of security should contact his or her Department Head, or the delegated representative, or IT.

2. IT will suspend all access for the authorized user in question pending a review and analysis of the security breach.

Questions regarding this policy should be directed to the Information Technology Help Desk.

2.