EMAIL ACCESS POLICY

INTRODUCTION

The Alabama Department of Postsecondary Education (DPE) email services support the administrative activities of the Department and serve as a means of official communication by and between users and DPE. The purpose of this policy is to ensure that this critical service remains available and reliable, and is used for purposes appropriate to the DPE mission.

1.0 – POLICY

1.1 Electronic Mail ("email") services shall be made available to every individual working at DPE for the purpose of conducting and communicating official Department business. Incidental personal use of email is allowed with the understanding that the primary use be job-related, and that occasional use does not adversely impact work responsibilities or the performance of the network.

1.2 Email services are provided only while a user is employed by DPE. Once a user is separated from DPE, the user's electronic services are terminated and former employees may no longer access the contents of their mailboxes, nor should they export their mailbox to a personal account before departure.

1.3 Email users are advised that electronic data (and communications using DPE network for transmission or storage) may be reviewed and/or accessed by authorized DPE officials for purposes related to Department business. DPE has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.

1.3.1 Email users do not have any expectation of privacy with regard to the contents of any such equipment, files or email on DPE's electronic systems.

1.4 Intentional and unauthorized access to other people's email is strictly prohibited.

1.5 Sending "spam", chain letters, or any other type of unauthorized widespread distribution of unsolicited mail is prohibited.

1.6 Use of email for non-Departmental-related commercial activities or personal gain is prohibited.

1.7 Use of email for partisan political or lobbying activities is prohibited.

1.8 Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications is prohibited.

1.9 Use of email to transmit materials in a manner which violates copyright laws is prohibited.

1.10 DPE attempts to provide secure, private and reliable email services by following sound information technology practices. However, DPE cannot guarantee the security, privacy or reliability of its email service. All email users, therefore, should exercise extreme caution in using DPE email to communicate confidential or sensitive matters.

1.11 Upon separation from DPE, an employee's mailbox will be made available to an authorized user who is assuming the separated employee's responsibilities for 45 days during which time the authorized

user should review and move any email messages containing institutional knowledge to his/her own mailbox. After 45 days the separated employee's mailbox shall be archived and be inaccessible.

2.0 – PROCEDURES

2.0 Employees should create an email account for personal use through a public service, such as the employee's internet service provider, Gmail, Hotmail or Yahoo. Personal emails should not be sent to DPE email accounts unless absolutely necessary (e.g., school system emergency alerts would be acceptable personal items to be sent to a DPE email account).

2.1 When sending information that may contain personally identifiable information (PII), the user must encrypt the message.

2.1.1 **Within DPE**: You can email PII without protection if the recipient's need for the information is related to his or her official duties. However, if you have any doubt about that, or to ensure protection, then you should password-protect the PII in a compressed file before you email within the Department. The password should be provided to the recipient in a separate form of communication (e.g., by phone, another email, or in person).

2.1.2 **Outside of DPE**: Email the PII within an encrypted, password protected, compressed attachment with the password provided to the recipient in a separate form of communication (e.g., by phone, another email, or in person).

2.1.3 **Directions to encrypt using PeaZip** (http://peazip.com/download/)

1. Save the file that needs to be encrypted.
2. Open up Windows Explorer and locate the file.
3. Right click on the file
4. Select **Peazip → Add to Archive**
5. The **Create .zip** dialog box will open
6. Click on **Enter Password/keyfile**
7. Enter in a **Password** and **Confirm** the password, ignoring the **keyfile** field. Press **OK.**
8. Press **OK.**
9. Your file is now encrypted in a compressed file (.zip) and you can attach the .zip file to your email.

2.2 Email users should be careful not to open unexpected attachments from unknown or even known senders, nor follow web links within an email message unless the user is certain that the link is legitimate. Following a link in an email message may execute code that can also install malicious programs on the workstation.

2.3 Forms sent via email from an unknown sender should never be filled out by following a link. Theft of one's identity can result.

2.4 Divisions that provide services in response to email requests should create an email distribution list to help support functional continuity for managing requests sent via email.

2.5 Users on an extended absence should create an Out Of Office message, which should include the contact information for another staff member who can respond while the user is away from the office.

2.6 An email account that has been compromised, whether through password-cracking, social engineering or any other means, must be promptly remedied with the appropriate means. The appropriate means will include a password reset, review of account settings, computer scans and malware disinfection to prevent possible leakage of PII, spamming, potentially infecting others and degradations of network service. If the account is being used to harm others and the owner cannot be reached in a reasonable period of time, the Director of Information Services may direct the resetting of the password.