Subject: Encryption Recommendations for Email File Attachments

The Maryland Higher Education Commission (MHEC) understands the desire of institutions to have the ability to email data files collected for the out of state registration renewal application to us. Since simple email attachments are not secure, the institution must consider safeguarding the Personally Identifiable Information in the email attachment containing the required data files. MHEC has in place an internal policy to adequately safeguard the data once it is in MHEC's possession. Until MHEC takes ownership of the data, the responsibility for security and privacy of data lies with the institution. The institution must adequately address the security and privacy of these data files both at their institution and during transport. With this in mind, MHEC makes the following recommendations to assist the institutions:

A. Do not attach files to email without some protection.

B. The level of protection can be decided by the school, but must be mutually manageable by both MHEC and the institution.

C. Passworded ZIP files from various ZIP software vendors that use the current ZIP 2.0 encryption standard are acceptable to MHEC. If the institution wishes to use this method of protection, MHEC will accept the passworded zipped file in email messages. Newer versions of ZIP software utilizing advanced encryption may not be compatible between vendors software.

D. MHEC will support one vendor's package for advanced encryption beyond current ZIP standard. The vendor MHEC has chosen is WINZIP. WINZIP software version 9.0 and greater will use the more robust advanced encryption techniques to protect data files.

E. The password or key can be telephoned to, sent by mail, sent in a separate email message, or delivered in person to the MHEC staff person responsible for the data survey: Jacqueline Cade (jcade@mhec.state.md.us).

F. If an institution chooses to use different encrypting software, it must be capable of producing self-extracting files and they must furnish the key via one of the methods above.

G. When sending self-extracting encrypted files to MHEC please change the file extension to .MHEC since our email system blocks files with an .exe extension. Be aware that you will be warned that changing the extension may make the file unusable. Click on OK when that warning is issued.

H. If an institution's security policy does not allow email transfer, we recommend the U.S. Postal Service, courier service or hand delivery by the institution staff.

I hope this provides you with recommendations that you can use in conjunction with your institution's security and privacy policies. Together these will guide you to the method most appropriate for your institution.