Mailman IT Alert, December 29, 2010

Did you know that it is against University policy to conduct School business with third-party, non-Columbia e-mail accounts? This includes using an e-mail account, such as Gmail or hotmail, as your de facto work e-mail, or even forwarding your Columbia e-mail to an outside e-mail provider. ([See official policy](#))

The reasons for this policy are simple, but the penalties for noncompliance are not:

1) As an institution that has been entrusted with public data, Columbia is legally obligated to ensure that our data is secure. While we can secure our internal e-mail systems, we have no control whatsoever over the security of third-party providers, which makes the risk of using them unacceptable. In fact, in the event of a data breach with an outside e-mail client like Google, the University/School is subject to financial penalties for not properly storing and policing sensitive e-mail data. Worse, **the faculty/staff person who sent and/or received the confidential data on that outside system is subject not only to University action, but to CIVIL PROSECUTION** by the government. As such, compliance with this policy actually protects *you.*

2) Some grantors (for example NIH) specify that no grant-related data be stored offshore from the US. However, currently most outside e-mail providers store data in world-wide data farms, and so far, refuse to agree to a strict domestic data storage arrangement. So, **use ofthese e-mail systems actually breaks many of our grantor requirements, and puts your hard work and grants at**

risk.

So, if you are currently using a third party e-mail system for work purposes, protect yourself by:

1) Switching immediately to your Columbia e-mail account

2) Moving any project-related data from third party providers to a Columbia system, such as your O drive.

3) Educating yourself as to the specific data storage requirements of your grants and other data security regulations, and recognize that CU systems are the only systems you can count on to be in compliance.
Thank you, Elizabeth Tashiro