Minimum Protection Policy for Restricted Information

Revision 11/13/2012

1. Purpose. The purpose of this policy is to establish minimum levels of protection for restricted data as defined in the USNH Data Classification Policy.

2. Scope. This policy applies to every student, faculty, and staff member at UNH, as well as any members of the general community working with or for UNH, who manages, receives, transmits or otherwise accesses university information.

3. Authority. This policy is maintained under the authority of the UNH Chief Information Officer.

4. Protection for Restricted Data: University Information for which protection is legally defined and/or it is required by federal and/or state law shall be protected in a manner that is consistent with the applicable law(s), established good information security and computing practices, and the following specific requirements:

   a. Restricted information shall not be stored on mobile devices. In cases where a legitimate business need exists to store restricted information on mobile devices, approval is required from the UNH CIO before proceeding. Persons who have this need must submit a request for approval through the Director of IT Security.

   b. Restricted information shall not be transmitted electronically in clear text form by electronic mail, through file transfer mechanisms, or other methods over the university network or through the Internet.

   c. Any personal computing device that is used to access restricted information or systems that contain restricted information shall be checked periodically for restricted data. If found, the data shall be immediately removed or secured in a manner that is consistent with university policy. Macintosh and Microsoft Windows computers are to be check with Identity Finder.

   d. The internal storage media in mobile devices that are used to access university systems and are at risk of loss, theft or unauthorized physical access shall be encrypted using the university approved and supported encryption service. Owners of these devices are responsible for ensuring that the devices are encrypted. Examples of devices are risk include but are not limited to personal computers that are transported outside of a secure office, left in parked vehicles, taken on business trips, taken home, or that are stored and used in office areas where others have unobstructed physical access to the device while it is not under the control of the owner. The currently approved and supported encryption service is Symantec PGP End Node Encryption.

   e. Mobile devices that are not compatible with the approved and supported encryption service shall be protected with available options, such as on-board encryption, strong password protection, automatic erase functionality following eight incorrect passwords, and remote wipe option. Owners of the devices are responsible for ensuring that these protections are enabled. To the extent possible, managers of central services that are accessed with such mobile devices will enforce the minimum protection for any devices that connects to that service.
5. Examples of restricted information include, but are not limited to Social Security Numbers, Medical Information, academic records, certain research results, and other personally identifiable information as defined by state or Federal laws.

6. Specific laws that contain additional data protection requirements include, but are not limited to, FERPA, HIPAA, FMLA, GLB, state privacy laws, research information that requires protection by law, and Information protected through "Affirmative Action" and/or "disability regulation".

7. Enforcement: This policy is enforced by the Director of IT Security under the guidance of the UNH Chief Information Officer. Any person that knowingly or willing violates this policy and continues to do so even after being alerted to the violation shall be subject to the university disciplinary process that may include revocation of access rights to the restricted information, re-assignment of duties and/or termination.