Server Protection Policy for the University of New Hampshire

Date of last revision of this document 7/6/2010

1. Authority
   1.1. This policy will be interpreted and enforced under the authority of the Chief Information Officer of the University of New Hampshire.

2. Rationale
   2.1. Compliance with this policy will aid in protecting the privacy and integrity of data created by and relating to all users of UNH IT resources and improve the availability of UNH IT resources.

   2.2. Compliance with this policy will aid in the protection of UNH’s computers and Network, and safeguard the data which they contain and transport from attack and compromise.

   2.3. UNH is compelled by law, USNH policy, and UNH CIO directive to assure appropriate protection of all Restricted UNH data. UNH also must protect certain Sensitive data and has a need to protect certain Public data as well. See the USNH Data Classification model for definitions.

   2.3.1. Federal Laws governing protection of UNH Restricted data include but are not limited to the following:
      2.3.1.1. Family Educational Rights and Privacy Act (FERPA) – Public Law 93-380
      2.3.1.2. Health Insurance Portability And Accountability Act (HIPAA) - Public Law 104-19
      2.3.1.3. Gramm-Leach Bliley Act (GLB) - Public Law 106-102
      2.3.1.4. Federal Trade Commission’s (FTC) Red Flags Rule - Section 114 of the Fair and Accurate Credit Transactions Act of 2003

   2.3.2. State of New Hampshire Laws include:
      2.3.2.1. RSA 359-C, RIGHT TO PRIVACY, Notice of Security Breach, Section 359-C:20

   2.3.3. UNH and USNH policies:
      2.3.3.1. Acceptable Use Policy for Information Technology Resources at the University of New Hampshire
      2.3.3.2. USNH Policy on Use of Technological Resources
      2.3.3.3. USNH Online Policy Manual Policy on Use of Technological Resources
      2.3.3.4. USNH Online Policy manual
      2.3.3.5. USNH Information System Access Policy
3. **Applicability**
   3.1. This Policy applies to every Server connected to any UNH Network.

   3.2. A Server is defined as any computing device connected to the Network which provides a service in response to unsolicited network traffic – e.g. a web Server, application server, print/file sharing server, email, etc. This includes devices containing financial, student, or employee records, as well as other information accessed from other devices over a network connection (i.e., through a mechanism other than from the console of the device storing the information). Exceptions from this definition for any short-lived equipment must be approved by the UNH CIO.

4. **Policy Statement**
   4.1. Every Server connected to any UNH Network must be registered as a Server with the operator of that Network.

   4.2. Every Server connected to any UNH Network must be properly maintained to prevent:
       4.2.1. Compromise of UNH information
       4.2.2. Harm to the UNH Network
       4.2.3. Harm to other equipment connected to the UNH Network or the Internet

   4.3. The manager of a department which owns or operates a Server will assign an administrator for each Server who will be responsible to insure Server registration and maintenance in accordance with this policy and in a manner that is consistent with the “Server Protection Process” available from it.security@unh.edu upon request.

   4.4. The managers/operators of the Network are responsible for monitoring and enforcement of compliance with this policy on their Network.

5. **Effective Date**
   5.1. This policy will become effective TBD.