UNH Guidelines for Safeguarding Privacy When Sharing Data With Third Parties

Media reports of security breaches at universities around the country have become all too common. Information security is an issue that UNH takes very seriously. UNH personnel have access to confidential information about students, parents, alumni, UNH employees and other participants in the UNH community, which may only be disclosed under appropriate circumstances. UNH’s obligation to protect the privacy of this information is governed by law (e.g., FERPA, HIPAA, Gramm-Leach-Bliley), as well as university policy. Examples of confidential information include social security numbers, credit card data, health and employment records, and any FERPA non-directory information about current or former students. Everyone at UNH has a responsibility for proper handling and protection of confidential information. In order to do so, each UNH community member must (i) be aware of the confidential information they have, (ii) understand who has access to it, (iii) understand all threats to its security, (iv) protect such confidential information, and (iv) assure that it is protected if they pass on confidential information.

One way that information security may be compromised is through the use of third parties to provide services. Examples include book publishers who offer online activities for students, vendors who support student response system technologies, online admissions processing companies, developers of systems for electronic processing of employee benefits, etc. To guard against illegal activity and to protect privacy, it is important that we use (i) systems and services already approved by and available from centrally-supported UNH departments and (ii) third-party vendors that we have contractually assured are aware of and responsible for meeting our data privacy requirements. UNH vendors dealing with confidential information must have a written contract covering their services, which must include a specific clause requiring the vendor to protect the data. For vendors being given access to certain high-risk data elements, the vendor’s security design, policies and procedures must be reviewed by UNH Information Technology.

Tips:
- Use existing UNH services and infrastructure; don’t agree to have confidential data stored outside of UNH’s control.
- Talk with UNH Information Technology about specific technology needs you have that are not currently available and/or supported by UNH.
- Protect the privacy of our students, employees, alumni and parents; don’t share information about them with a third party except as allowed by law.
- Keep your electronic devices (laptops, desktops, servers, PDA’s, flash drives, CDs etc.) secure - don’t leave devices where they could be stolen or hacked, and use encryption technology when available.
- Keep your own UNH ID and password safe -- don’t share it with colleagues or third parties.
- Consult with UNH Information Technology and/or the USNH General Counsel’s Office regarding contracts that involve handling of (or access to) confidential information of students, employees, alumni or parents.

Guidelines and Questionnaire for Vendors

These guidelines help ensure that sourcing from third-party vendors of services which could result in the disclosure of personally identifiable confidential information about UNH students, employees, alumni, parents or other community members complies with UNH protocols for data privacy protection. Such services may include (but are not limited to), off-campus hosting of electronic services provided by UNH sites and any third-party service provided by link from a UNH site.

1. UNH Technology Vendor Guidelines - see next page.
3. Other procurement guidelines - see http://www.unh.edu/purchasing/ and your BSC.

Any questions about technology to protect confidential information should be directed to UNH Information Technology. These links provide information about some of UNH’s obligation to protect
confidential information under applicable law and university policy: FERPA; HIPPA (Research); HIPPA (HR); Health Services Privacy Practices; other or UNH links]. Also see http://it.unh.edu/itsecurity.
UNH Technology Vendor Guidelines

General

1. Non-UNH parties wishing to provide externally-hosted educational applications for UNH faculty and students must first be approved by the Director of Academic Technology.

2. Non-UNH parties wishing to provide externally hosted applications (other than educational applications) for UNH must first be approved by the UNH IT Security Officer.

3. Vendors should provide a copy of their privacy policy and user agreements that apply to the technologies and services involved.

4. To ensure that the University has at least the minimum amount of information needed to evaluate whether the application meets the University’s policies and needs, vendors will be asked to provide basic information addressing specific areas of concern outlined in the “UNH Technology Vendor Questionnaire” and “Application Service Provider Standards” files.

5. The principal points that the University will consider concern overlap with existing campus systems, privacy, security, data retention, compatibility, and support.

6. Students and faculty should be provided with free and convenient support.

7. Any direct costs to students, faculty, or the University must be specified.

8. Vendors must agree not to share or sell personal information collected from UNH users with any third parties, unless the UNH users affirmatively agree to such sharing in response to a conspicuous and clear request from the vendor.

Privacy

1. Vendors should be aware of, and fully compliant with legal privacy requirements (e.g., FERPA, HIPAA, and Gramm-Leach-Bliley) and industry standards (e.g., PCI data standards).

2. Unless a UNH user needs to pay for portions of the application by credit/debit card, they should only be required to provide their name and an email address when registering for or using the application. They should not be required to provide their student number or SSN.

3. For educational applications, students and faculty in one course must not be able to see identifiable information (including names) of students in another course.

4. For educational applications, tools and content areas should be able to be turned off or restricted by the instructor, both to allow shutting off areas that may violate UNH’s policies with regard to FERPA and to prevent confusion with tools that duplicate functionality already provided by the University.

5. When registering or logging in for the first time to non-UNH sites, UNH users must be notified that they are on a non-University site.

Security

1. When the systems include data that raise security and privacy concerns, UNH prefers to host applications on campus when feasible. The availability to host locally may affect decisions about the use of an application.

2. UNH should be informed when a vendor uses a third party to host or develop applications. Third-party hosting may be a factor in decisions about using an application.
3. All data transmissions containing personally identifiable confidential information or other sensitive data shall be encrypted. All transmission protocols used between systems shall be explicitly indicated.

4. One-way, pass-through authentication from Blackboard or WebCT is preferred. If it is not available, a supported campus authentication service (such as Blackboard Single Sign-on) is preferred to vendor-only authentication solutions. In the case of a vendor provided authentication scheme, vendors shall provide information on the requirements and management practices associated with usernames and passwords.

5. For off-campus hosted solutions, the vendor shall provide information related to vulnerability management of their networks, systems and applications as well as appropriate documentation to support the vendor’s use of defense in depth strategies related to information security for their product.

Data Retention

1. UNH has data retention protocols that require preservation and destruction of student and employee data at specified times. The vendor shall provide information related to the vendor’s preservation and destruction UNH data, and will provide UNH with a means of obtaining that data for retention.

2. Vendors should provide information on their backup and restoration policies and procedures, including details of what data are retained, who has access to it, and what steps are taken to ensure privacy law compliance.

Compatibility

1. Vendors will need to provide information about the compatibility of their applications with different operating systems. Minimum versions of operating systems, browsers, plug-ins, or other required software (or of hardware) must be provided.

2. The application must be ADA compliant.